S. HRG. 112–242

CYBERSECURITY AND DATA PROTECTION IN THE FINANCIAL SECTOR

HEARING

BEFORE THE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

ON

EXAMINING CYBERSECURITY AND DATA PROTECTION IN THE FINANCIAL SECTOR

JUNE 21, 2011

Printed for the use of the Committee on Banking, Housing, and Urban Affairs

Available at: http://www.fdsys.gov/

U.S. GOVERNMENT PRINTING OFFICE

72–701 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

TIM JOHNSON, South Dakota, *Chairman*

JACK REED, Rhode Island
CHARLES E. SCHUMER, New York
ROBERT MENENDEZ, New Jersey
DANIEL K. AKAKA, Hawaii
SHERROD BROWN, Ohio
JON TESTER, Montana
HERB KOHL, Wisconsin
MARK R. WARNER, Virginia
JEFF MERKLEY, Oregon
MICHAEL F. BENNET, Colorado
KAY HAGAN, North Carolina

RICHARD C. SHELBY, Alabama
MIKE CRAPO, Idaho
BOB CORKER, Tennessee
JIM DEMINT, South Carolina
DAVID VITTER, Louisiana
MIKE JOHANNS, Nebraska
PATRICK J. TOOMEY, Pennsylvania
MARK KIRK, Illinois
JERRY MORAN, Kansas
ROGER F. WICKER, Mississippi

DWIGHT FETTIG, *Staff Director*
WILLIAM D. DUHNKE, *Republican Staff Director*

CHARLES YI, *Chief Counsel*
DEAN SHAHINIAN, *Senior Counsel*
LAURA SWANSON, *Policy Director*
PAT GRANT, *Counsel*
LEVON BAGRAMIAN, *Legislative Assistant*

DAWN RATLIFF, *Chief Clerk*
BRETT HEWITT, *Hearing Clerk*
SHELVIN SIMMONS, *IT Director*
JIM CROWELL, *Editor*

C O N T E N T S

TUESDAY, JUNE 21, 2011

	Page
Opening statement of Chairman Johnson	1
Prepared statement	24
Opening statements, comments, or prepared statements of:	
Senator Reed	2
Senator Menendez	2

WITNESSES

Kevin F. Streff, Associate Professor of Information Assurance, Dakota State University Information Assurance Center	3
Prepared statement	24
Stuart K. Pratt, President and Chief Executive Officer, Consumer Data Industry Association	5
Prepared statement	35
Leigh Williams, BITS President, on behalf of the Financial Services Roundtable	6
Prepared statement	38
Marc Rotenberg, Executive Director, Electronic Privacy Information Center	8
Prepared statement	45
Pablo Martinez, Deputy Special Agent in Charge, Criminal Investigative Division, Secret Service	9
Prepared statement	57

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

Statement submitted by the Securities Industry and Financial Markets Association	63

CYBERSECURITY AND DATA PROTECTION IN THE FINANCIAL SECTOR

TUESDAY, JUNE 21, 2011

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
Washington, DC.

The Committee met at 10:01 a.m., in room SD–538, Dirksen Senate Office Building, Hon. Tim Johnson, Chairman of the Committee, presiding.

OPENING STATEMENT OF CHAIRMAN TIM JOHNSON

Chairman JOHNSON. The Banking Committee will come to order. The Banking Committee meets today to hear testimony about data protection and cybersecurity issues in the financial sector.

Over the past 12 years, the Committee has enacted several pieces of legislation to protect consumer data held by financial institutions. Federal financial regulators under the Committee's jurisdiction have issued extensive rules and guidance on data practices that require the institutions they regulate to keep data secure, notify customers and regulators when breaches occur, authenticate customers, and notify customers about how their sensitive information may be used.

Recent high-profile data breaches at major institutions within the financial sector and elsewhere underscore the importance of cybersecurity for the American economy. Breaches are disruptive and raise the potential for financial fraud, identity theft, and, potentially, severe threats to our national economic security. This is an important issue that deserves the Committee's careful attention and continued oversight.

Today I invite the witnesses to share their views in three areas: the current regulation of data practices affecting financial institutions and their customers; the current state of data privacy protection, data breaches, and cybersecurity in the financial sector; and how legislative proposals, such as the Administration's cybersecurity bill, would affect financial institutions and would interact with existing regulation.

I look forward to the testimony of our witnesses and to the question-and-answer period.

Are there any other members who would like to give opening remarks?

Senator REED. Mr. Chairman?

Chairman JOHNSON. Senator Reed.

STATEMENT OF SENATOR JACK REED

Senator REED. Mr. Chairman, just very briefly, I want to commend you for holding this very timely hearing. The cyber dimension is something that is evolving so quickly, huge consequences not just in the realm of financial information but in national security policy. It is almost as if we are sort of in the same position our predecessors were in 1920 trying to figure out how to use the airplane, where it was a novelty or a fundamentally game-changing—obvious it was fundamentally game changing. So thank you, Mr. Chairman, for your thoughtful hearing.

Chairman JOHNSON. Senator Menendez.

STATEMENT OF SENATOR ROBERT MENENDEZ

Senator MENENDEZ. Thank you, Mr. Chairman. Briefly, I want to joint Senator Reed in thanking you for holding this hearing, something I have been very interested in pursuing in my legislation on the Cybersecurity Enhancement Act.

I am concerned—and certainly the Committee's jurisdiction is very appropriate here when financial institutions face major breaches, and I am concerned about what are the financial institutions doing, number one, to enhance their position against cybersecurity attacks; and, number two, when there is a breach, what are they doing in their fiduciary responsibility to notify their customers of those breaches.

It just happens that my chief of staff was one of those individuals whose information was breached under the City cyber attack. Now, unfortunately, he was not notified, and it was not until he attempted to use his card and found out that it was impossible for him to use it and eventually called Citi that he found out that, in fact, his information had been breached.

Now, it seems to me that there is a fiduciary responsibility by the entity to proactively tell their customer that, in fact, that has happened. And it strengthens, I believe, the institution at the end of the day to be honest and forthcoming as well as it gives the customer, the consumer, the wherewithal to protect themselves as well.

So I look forward to hearing some of the expertise of these witnesses, Mr. Chairman, and working with you to move to a more secure process for all of our customers, all of our consumers, all of our constituents.

Chairman JOHNSON. Now I would like to welcome the witnesses for our panel today.

Dr. Kevin Streff is a good friend from South Dakota. He is an associate professor and director of the Center for Information Assurance at Dakota State University.

Mr. Stuart Pratt is the president and CEO of the Consumer Data Industry Association.

Mr. Leigh Williams is the president of BITS, a division of the Financial Services Roundtable.

Mr. Marc Rotenberg is the president of the Electronic Privacy Information Center.

And Mr. Pablo Martinez is deputy special agent in charge in cyber operations at the Criminal Investigative Division of the U.S. Secret Service.

I thank all of you again for being here today, and I look forward to your testimony. I will ask the witnesses to limit your remarks to 5 minutes. Your written statements will be submitted for the record.

Dr. Streff, would you like to begin?

STATEMENT OF KEVIN F. STREFF, ASSOCIATE PROFESSOR OF INFORMATION ASSURANCE, DAKOTA STATE UNIVERSITY INFORMATION ASSURANCE CENTER

Mr. STREFF. Chairman Johnson, Ranking Member Shelby, and Members of the Senate Committee on Banking, Housing, and Urban Affairs, thank you for the opportunity to testify to the need for comprehensive cybersecurity legislation and in support of the Administration's cybersecurity proposal. I am pleased to appear before you today on behalf of the National Center for the Protection of the Financial Infrastructure at Dakota State University to share our views on security in small- and medium-sized financial institutions. My name is Dr. Kevin Streff, and I am director of the NCPFI, whose mission is to advance the security and safety of the Nation's electronic financial infrastructure.

Eighty-five percent of the U.S. electronic infrastructure is owned and operated by the private sector. PDD 63 identified financial services as a critical infrastructure, advising a public–private partnership model whereby the public sector partners would partner with the private sector infrastructure owners to secure it. While there has been much effort, the results are insufficient to safeguard this infrastructure.

Cybersecurity laws for financial services have been enacted, including Gramm-Leach-Bliley, Bank Secrecy Act, USA PATRIOT Act, identity theft red flags rule, and Sarbanes-Oxley. PCI has also been established at a data security standard for card information.

SMFIs, small- and medium-sized financial institutions, operate in a complex regulatory environment with community banks regulated aggressively and credit unions less. We encourage care in setting the new CNCI regulation to fit with the good work of the banking regulators.

Over 300 million data records impacting financial services have been breached since 2005. When terrorists target these SMFIs and small- and medium-sized businesses, SMEs, they will find a soft underbelly of underprotected targets. I recently completed a study and found that 70 percent of small- and medium-sized businesses lack basic security controls. *Information Week* states SMFIs and SMEs have a wealth of data that cybersecurity thieves are targeting with increased regularity. White House Cybersecurity Coordinator Howard Schmidt recently stated that 85 percent of cyber attacks are now targeting small businesses.

Technology is advancing faster than SMFIs can secure. For example, a picture of a check from a cell phone camera can be deposited in a consumer's account. Consumers are demanding mobile and social media technologies. The risk profile 10 years ago included a teenager breaking into computers for fun, while the risk profile today is a professional breaking into networks, cell phones, laptops, mobile devices, social media sites, merchants who deposit checks via imaging systems, service providers who host critical

banking applications, and Web sites that validate flood plains and credit bureau information. With the mounting risks of offshoring, requiring data centers to be located in the U.S. seems good policy in increase our cybersecurity posture.

SMFIs and SMEs lack security experts, unable to access and afford qualified security specialists who command six-figure salaries. Therefore, a SMFI will typically name a loan officer or a VP of Operations or their IT staff their information security officer. Understanding emergent security threats and threat actors and vulnerabilities takes expertise and simply cannot be assigned to existing staff. Universities, community colleges, and trade schools can do more to produce security experts that can work in these environments.

We applaud the President for including CNCI Initiative Number 8, Expanding Cyber Education. We commend the Government for anticipating the cybersecurity issue and resource shortage back in 2001 when the NSA began designating Centers of Academic Excellence. Today 106 universities are designated Centers of Academic Excellence, and we encourage the President to consider expanding this program with funding so that more educational research and outreach opportunities are created to serve the needs of Government and industry, including small- and medium-sized companies.

The Financial Services Sector Coordinating Council has led the development of a formal research agenda necessary to improve the security of the electronic infrastructure. However, funding is, again, lacking to make significant progress. Other research funds, such as NSF, SBIR, and the like, could be augmented to carry out the Treasury's agenda.

To the degree that major changes are needed at SMFIs and SMEs, we urge the Administration to consider this infrastructure and defense and fund it. If this infrastructure is a matter of national security, then the Government may have a funding responsibility, and just as roads are infrastructure, networks are cyber infrastructure. Just as tanks and weapons are funded to protect our defense interests, we urge the Administration to consider its financial responsibility as it relates to cyber defense.

President Obama said it best: "We count on computer networks to deliver our oil, our gas, our power, and our water. But we have failed in the past to invest in our physical infrastructure, and we are failing now to invest in our digital infrastructure. The *status quo* is no longer acceptable."

Electronic banking is the future. NCPFI and Dakota State University look forward to working with all stakeholders to operationalize the President's vision of a safe electronic infrastructure for all businesses. We applaud the President in making cybersecurity an Administration priority and concur with the President's comments that the "cyber threat is one of the most serious economic and national security challenges we face as a Nation."

Thank you

Chairman JOHNSON. Thank you, Dr. Streff.

You may proceed, Mr. Pratt.

STATEMENT OF STUART K. PRATT, PRESIDENT AND CHIEF EXECUTIVE OFFICER, CONSUMER DATA INDUSTRY ASSOCIATION

Mr. PRATT. Chairman Johnson and members of the Committee, my name is Stuart Pratt, and I am president and CEO of the Consumer Data Industry Association. Thank you for this opportunity to testify.

Let me start with an overview of some of the most relevant laws and regulations which impose data security duties on the financial institutions today.

One of the most pressing actions of the Committee was the 1999 passage of Title V of the Gramm-Leach-Bliley Act, signed into law by President Clinton. Title V directed bank regulatory agencies and the Federal Trade Commission to develop regulations regarding the security of nonpublic personal information. These rules are flexible but do require financial institutions of all sizes to implement a written information security program, conduct risk assessments, and to do so periodically in order to update these programs.

In 2003, the Committee amended the Fair Credit Reporting Act to require proper disposal of consumer information or any compilation of consumer information derived from consumer reports. This straightforward duty ensured that sensitive personal data about consumers was not simply left in a dumpster or on a hard drive of a laptop or a hand-held device which was sold without concern for the contents.

As a result of this Committee's actions to enact both FCRA and GLB, our members have a number of duties to ensure that they also know their customers, which is yet another important part of ensuring that a full and complete data security program is in place. This is an area in which our members invest heavily.

With this baseline of law in mind, you also asked us to comment on how proposals such as the Administration's cybersecurity bill would affect financial institutions that come under the Committee's jurisdiction. The key to successful cybersecurity initiatives is to ensure alignment between existing statutory and regulatory regimes and those that are new.

CDIA believes that while it is absolutely and unequivocally appropriate for the Administration and Congress to focus on the ever changing mix of risks posed by cybersecurity threats, it is also important for new laws not to impinge on frameworks of law that are already established and create the necessary focus on data security. We urge Congress to consider the data security standards in GLB as the model for data security requirements for other sectors of the U.S. economy.

Forty-eight States have enacted data breach notification laws, and some financial regulatory agencies have established guidance on this topic for those within their jurisdiction. While CDIA is on record as supporting a national standard for data breach notification, any new requirements resulting from efforts to address cybersecurity risks should not interfere with the direction of this investment, which requires multiyear planning.

In focusing on cybersecurity risks, Congress should not be distracted by privacy issues that are not relevant to data security. Several congressional committees have delved into this privacy

arena in an effort to address the data collection and use practices of so-called information brokers. Under these proposals, our members' products and services, which are particularly essential to the financial services sector, could be adversely affected. Consider the following:

Financial institutions offering credit need to detect and prevent fraud and to verify the identities of individuals seeking products and services.

Financial institutions must enforce contracts with customers who have the ability to pay but do not choose to do so.

Lenders, who must comply with Bankruptcy Code requirements to cease dunning a consumer, use our members' tools in order to comply. USA PATRIOT Act Section 326 duties and FACT Act red flag guidelines demand that financial institutions properly identify their customers.

Even President Obama's National Strategy for Trusted Identities in Cyberspace will likely rely on our members' current and emerging identity verification tools. It is our members' products and services that empower the financial services sector to protect consumers and comply with current laws.

In closing, we applaud both the Congress and the Administration's focus on cybersecurity risks. We believe that this work must, however, be careful not to impair or impinge on effective laws that already address risks in the financial services sector. Alignment is key.

I am happy to answer any questions. Thank you.

Chairman JOHNSON. Thank you, Mr. Pratt.

Mr. Williams.

STATEMENT OF LEIGH WILLIAMS, BITS PRESIDENT, ON BEHALF OF THE FINANCIAL SERVICES ROUNDTABLE

Mr. WILLIAMS. Thank you, Chairman Johnson and Members of the Committee. My name is Leigh Williams, and I am president of BITS, the technology policy division of The Financial Services Roundtable. BITS addresses technology policy on behalf of its 100 member institutions, our millions of customers, and all of the stakeholders in the U.S. financial system.

In my remarks today, I will briefly describe cybersecurity protections in financial services and explain why the Roundtable supports the Obama administration's cybersecurity proposal.

In my view, most cybersecurity protection arises from individual institutions investing tens of billions of dollars and tens of millions of hours in voluntary measures for business reasons. Up at the industry level, BITS and several other coalitions promote best practices for protecting customer information. For example, BITS is currently addressing security in mobile, cloud, and social networking, protection from malicious software, security training and awareness, and the prevention of retail and commercial account takeover.

Beyond these voluntary efforts, our members are also subject to a range of oversight mechanisms to ensure consistency throughout the industry. Just to take the security and privacy provisions of Gramm-Leach-Bliley as an example, this Committee and the Congress enacted GLB. The regulators detailed it in Regulation P. Reg-

ulation P was translated into guidance. Institutions used that guidance to manage their programs. Examiners audit the programs. Treasury monitors for consistency. And just to take this whole process full circle, this Committee oversees Treasury and the agencies.

Beyond this sector-specific work, we collaborate more and more in public–private and in financial–nonfinancial partnerships, often with regulators, DHS, with law enforcement, with the intelligence community, and others.

People are not just consumers or just customers or citizens. They are all of these. So business and Government are working together to protect e-commerce and national economic security.

As the Committee considers action on cybersecurity, I urge members to appreciate these existing protections and these current collaborations and to leverage them for maximum benefit.

Even given this head start, we believe that comprehensive cybersecurity legislation is warranted. It can improve security throughout the cyber ecosystem, including in the telecom networks on which our financial institutions depend, and it can strengthen the security of Federal systems and mobilize law enforcement resources.

More specifically, the Roundtable supports the Administration's legislative proposal. We support many of the provisions on their own merits, and we see the overall proposal as an important step toward building a much more integrated approach.

The Administration's proposal has this comprehensive approach. It addresses cybersecurity both at the level of the entire ecosystem and also within specific sectors like financial services. For example, the law enforcement title refers to damage to critical infrastructure computers, but also to wire fraud and mail fraud. The breach notification title refers to sensitive personally identifiable information and FTC enforcement, but also to financial account numbers and credit card security codes.

We believe that harmonizing this comprehensive approach and the sector-specific mechanisms will be an important challenge as the Congress considers this proposal. There are at least a couple of ways of bridging this ecosystem/sector divide.

First, the Congress could establish uniform standards but allow for exceptions where substantially similar requirements are already in place, as in the FFIEC agencies' breach notification requirements. Or the Congress could reserve more autonomy for the sectors. For example, it could be the sector-specific agencies and not DHS that determine what entities are critical, much as in our sector the sector authorities designate the systemically important financial institutions.

In conclusion, may I just say that at the Roundtable we will continue to strengthen security protection around our customers' information. We will help to answer this question of ecosystem/sector balance, and we will support and work to implement the Administration's cybersecurity proposal.

Thank you very much for your time.

Chairman JOHNSON. Thank you, Mr. Williams.

Mr. Rotenberg.

STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. ROTENBERG. Thank you, Mr. Chairman and members of the Committee. My name is Marc Rotenberg. I am president of the Electronic Privacy Information Center. I also teach privacy law at Georgetown Law Center. I am grateful for the opportunity to testify today and also for your interest and the Committee's interest in this particular issue.

No doubt you have been reading the news stories and the growing accounts of data breaches affecting bank customers across the country. Just recently, Citigroup had to admit that more than 360,000 of their customers had their personal information improperly accessed. Bank of America was reported to have lost customer information, resulting in the loss of millions of dollars to their customers, though it took them more than a year to acknowledge this.

The Identity Theft Resource Center reports that in 2010 there were 662 security breaches; 58 of those occurred at financial institutions. And we believe this problem is going to get worse. More of our personal information is moving into cloud-based services, being stored on remote computing systems. Bank customers know less and less about the information about them that is being collected or how it is being used, which is why data breach notification becomes so very important so that customers understand the risks that they have been exposed to.

This is not just the problem of identity theft, though to be sure that is a serious problem. According to the Federal Trade Commission, identity theft has been the number one concern of American consumers for the past decade. But as we learned in the recent Citigroup breach, there is also the problem of phishing, which is the use of bits of personal information to obtain other bits of personal information. So even without the bank account number, to have access to the bank account name can be sufficient to then begin the process that leads to other types of crimes against individuals.

Now, in my testimony, I have gone into some detail about the current Federal legislation as well as the State laws and the White House cybersecurity proposal, and if I may, I would like to highlight just a few of the key points now.

The first thing to be said is that the privacy provisions in Gramm-Leach-Bliley do not adequately address these new challenges. They do not give customers the type of notification that they need to respond when these problems arise. Many of the States, we believe, have actually done a good job in trying to promote data breach notification so that customers are aware of these risks. And, of course, in consideration of Federal legislation, we would be concerned about bills that might preempt these strong State measures.

The experience in California, which I describe in my testimony, is particularly significant because it was that State breach notification law that made is possible for the Government to act upon information that the personal information on American consumers had actually been sold to a criminal ring engaged in identity theft. I think without that State law that problem would have never

come to light, and the authorities would not have been able to pursue the investigations.

Now, turning to the White House cybersecurity proposal, we are broadly in favor of many of the recommendations from the White House. They have clearly treated this issue as a priority, and they have tried to develop a comprehensive approach that deals with the many different dimensions of cybersecurity. We do not object to the role of the Department of Homeland Security in promoting the strengthening of security safeguards for American business, but we would caution against overreaching because there is always concern that if the Government sets technical standards in such areas as intrusion detection or intrusion prevention, there is some risk that there will be increasing surveillance and monitoring of the private communications of American citizens. But as I said at the outset, their approach to cybersecurity we think is a good one, and it is in a cooperative relationship between the public sector and the private sector can help address some of the risks that American customers are today experiencing.

We would also note that there are other bills that have been introduced in both the Senate and the House that try to establish new safeguards for customers. We think, for example, the private right of action is an important right to ensure that in the absence of effective oversight by the regulatory agencies, individuals who do suffer harm as a result of these breaches are given the opportunity to pursue their rights as well.

Finally, in our statement we draw attention to some of the new security techniques that we had previously recommended in the communications field, and we think they would be helpful in the financial sector as well. In particular, the goal of minimizing the collection of personal data not only reduces the attractiveness of a target to hackers and to others, but when a breach does occur, the subsequent damage is limited as well. So we continue to promote efforts within the legislative process that favor the minimization of data collection.

Thank you again for the opportunity to testify. I would be pleased to answer your questions.

Chairman JOHNSON. Thank you, Mr. Rotenberg.

Mr. Martinez.

STATEMENT OF PABLO MARTINEZ, DEPUTY SPECIAL AGENT IN CHARGE, CRIMINAL INVESTIGATIVE DIVISION, SECRET SERVICE

Mr. MARTINEZ. Good morning, Chairman Johnson and distinguished Members of the Committee. Thank you for the opportunity to participate in this morning's hearing.

The Secret Service was established as an investigative bureau of the Department of Treasury in 1865 in response to the proliferation of counterfeit U.S. currency. While most people today associate the Secret Service with the protection of the President, it was not until 1901 that our agency was charged with that mission. Our dual mission of investigations and protection has evolved over the course of the last century, not because we seek new responsibilities, but because the criminal methods used by our adversaries are constantly evolving.

Over the past decade, Secret Service investigations have revealed a significant increase in the quantity and complexity of cyber crime cases. Broader access to advanced computer technologies and the widespread use of the Internet has fostered the proliferation of computer-related crimes targeting our Nation's financial infrastructure. Current trends show an increase in network intrusions, hacking attacks, malicious software, and account takeovers resulting in data breaches affecting every sector of the American economy.

In recent years, the Secret Service has been responsible for the arrest of numerous transnational cyber criminals who are responsible for the largest network intrusion cases ever prosecuted in the United States. These intrusions resulted in the theft of hundreds of millions of account numbers and a financial loss of approximately $600 million to financial and retail institutions, directly impacting the lives of millions of American citizens.

The 31 Electronic Crime Task Forces that the Secret Service has established domestically and abroad exemplify the Secret Service's commitment to sharing information and best practices. Membership in these ECTFs includes more than 4,000 private sector partners, nearly 2,500 international, Federal, State, and local law enforcement officials and more than 350 academic partners. The Secret Service continually develops the technical expertise to track down and successfully infiltrate, investigate, and prosecute with our partners cyber criminals who pride themselves on their knowledge and technical prowess. We use this knowledge of criminal networks to adapt our response to the challenges posed by financial crimes in the 21st century.

A central component of our approach is the training provided through our Electronic Crimes Special Agent Program, which gives our special agents the tools they need to conduct cyber-crime-related investigations. The training we provide, however, extends past our own agents to others in the public sector. We continue to train State and local law enforcement through the National Computer Forensics Institute. The goal of this facility is to provide our partners with the necessary training not only to understand cyber crime, but to respond to any type of cyber-related investigation. Since 2008, we have provided training to 932 State and local law enforcement officials, prosecutors, and judges.

Investigations continue to highlight the need for further collaboration between the financial services industry and law enforcement. In recent years, the Secret Service, in collaboration with the Department of Treasury, has briefed organizations such as the Federal Reserve Board, the Securities and Exchange Commission, the Federal Deposit Insurance Corporation, as well as private sector organizations such as the Financial Services Information Sharing and Analysis Center, Securities Industry and Financial Markets Association, payment card processing industry, and the payment card industry on the latest trends and threats to their networks and operations. These briefings have occurred within the Beltway, but also across the country through our nationwide network of Electronic and Financial Crimes Task Forces.

The legislative package proposed by the Administration will better equip law enforcement agencies, such as the Secret Service, with the additional tools to combat transnational cyber crime by

enhancing penalties against criminals that attack critical infrastructure and adding computer fraud as a predicate offense under the Racketeer Influenced and Corrupt Organizations Act. With regard to data breaches, it will replace the patchwork of State laws governing reporting of breaches of personally identifiable information with a uniform standard requiring businesses to notify affected individuals and the Government if the business suffers a breach.

Chairman Johnson and distinguished Members of the Committee, the Secret Service is committed to our mission of safeguarding the Nation's financial infrastructure and will continue to aggressively investigate cyber and computer-related crimes to protect American consumers and institutions from harm.

This concludes my prepared statement. Thank you for the opportunity to testify at this Committee.

Chairman JOHNSON. Thank you, Mr. Martinez.

Professor Streff, you have testified that smaller banks know their customers better than large banks, but do not have the same resources to spend on protecting customer information. How do small banks work to ensure that their customers are protected, and what can the Federal Government do to aid these small businesses?

Mr. STREFF. Thank you for the question. What small- and medium-sized financial institutions do is, really, they comply with the IT Examination Handbook, which is ten booklets of about 1,000 pages that—it is out there on FFIEC.gov, and they put a comprehensive information security program in place that starts with risk assessment, identifies business continuity issues, pandemic preparedness issues. They hire somebody to break into their networks. They scan their networks from the inside, a whole host of different programs. Then an independent organization comes in and audits and verifies that their information security program is, indeed, in and working effectively.

So there is already a lot done in place now. So that is where, when we see more and more of these requirements coming down, we want to make sure that what the Federal Government can do is make sure that what comes out fits nicely with what is already there. The FDIC, the OCC, and others work very hard with fills and regulatory insights and other pieces of guidance to interpret the law and to get it out there in a way that these small- and medium-sized financial institutions can operationalize effectively.

Chairman JOHNSON. For all the panelists, community banks and rural banks currently meet stringent data security standards. How would the Administration proposal affect community and rural banks and their regulatory burden?

Mr. PRATT. Mr. Chairman, I think, and this really applies to anyone who falls under the various laws that I think a number of us have talked about here at the table today, what is most important is to ensure that if you are a community bank or a smaller financial institution, and candidly, even if you are one of the largest in the country, that you have some continuity in terms of those who are going to examine you. They have expertise. They understand how the financial services marketplace works.

So I think it is critically important that you preserve that base of knowledge that you have with bank agencies, with examination processes, in our case, with the Federal Trade Commission, who

continues to retain data security responsibilities for enforcement of various provisions of the Fair Credit Reporting Act, but also Gramm-Leach-Bliley. These agencies have that expertise.

What you would not want is some sort of regulatory overlap between what you have today and a DHS designation of a critical infrastructure element where a bank or—small or large—has to struggle with yet another set of requirements which may not necessarily advance the ball in terms of security, but just will necessarily require them to comply with, potentially, two different competing approaches to security. So I think that alignment issue we talked about before is very important.

Chairman JOHNSON. Anybody else?

Mr. WILLIAMS. Mr. Chairman, I certainly believe in everything that Professor Streff and Mr. Pratt have said about alignment. That is absolutely critical.

We see the proposal as doing two new things. One is it better aligns what already happens in financial services, which admittedly is imperfect, is evolving, and which continues to be improved at both the institution and at the industry level, but now could be better connected with the rest of the ecosystem with efforts at the Internet Service Providers, the software manufacturers, with what happens out at our customers' PCs. We believe that the overall ecosystem approach contemplated in this new proposal begins to connect these existing safeguards in our industry to what needs to happen throughout the ecosystem.

The second major change is that it is not only across industries, but it is across the public and private sectors. So Federal systems are also covered. Information sharing with the Government is also covered. We think there would be much better collaboration between institutions and industry and Government partners that can bring expertise and resources to the table.

Chairman JOHNSON. What are the witnesses' views on the effectiveness of the Federal financial regulators under this Committee's jurisdiction in administering laws affecting data protection and data security? Anybody?

Mr. ROTENBERG. My view, Mr. Chairman, is that the laws currently in place do not provide adequate protection to bank customers, particularly in light of some of the recent security breaches that have been so widely reported. We make several recommendations for how those laws might be strengthened, but we also point out that as the law was written, it operated as a Federal baseline and that allowed the States to regulate upward where they saw the need to do so. We think that is a good approach. We think it allows the States to put in place stronger safeguards and to continue to innovate as some of these new challenges emerge.

Mr. WILLIAMS. Mr. Chairman, if I might, I absolutely agree with Mr. Rotenberg's comment that GLB and some of the other regulations are largely established as a baseline. But rather than think about State intervention to move higher, we tend to think of self-regulatory and business practices as pushing practices well beyond that baseline. So if, as part of this initiative, or if, as evolving regulation raises the bar, we also very much will focus on institutions and industries stepping in and voluntarily raising the bar in what we think is the most dynamic approach.

Mr. STREFF. If I could comment, as well, I think the comprehensive approach will promote consistency. If the breach happens at the bank, then the notification will happen a certain way. If it happens at a credit union, it will happen a certain way. If it happens at a trusted vendor, it will happen a certain way. If it happens at a merchant or a small business as part of a corporate account fraud that we are seeing, it happens a certain way. I would think that the consumers today are confused with when they are notified, how they are notified, due to the inconsistencies and the lack of a comprehensive approach.

Mr. MARTINEZ. Chairman Johnson, I would agree with the comments made here today. Working data breach cases for over 5 or 6 years now, we have seen all the different levels of financial institutions that have been victims of data breaches, and I believe a uniform standard across the Nation would be a more effective way of moving forward.

I also believe that it is incumbent on businesses to notify victims that have been—or individuals that have been victimized from a data breach and also to notify law enforcement. I think it is important that we try to do a coordinated effort when moving forward on some of these data breach investigations.

Mr. PRATT. Mr. Chairman, I would just like to add, this uniformity is critically important and I would agree with Mr. Williams' statement that industry itself is deeply motivated to protect the information that it has and they design multiyear budgets to build out, not just simply to sustain or to meet the minimal baseline, but to develop the best systems that industry can buy. But it is critically important that we are able to build these on the nationwide basis.

That is just not important for the largest companies, but it is also important, actually, for the smaller companies that want to compete on a regional or super-regional basis. The more complicated the statutory structure is, the more difficult it is for them to have the resources to even approach compliance on a State-by-State basis. So CDI has been on record as very supportive of a national standard for data breach notification, for example.

Chairman JOHNSON. Senator Reed.

Senator REED. Well, thank you very much, Mr. Chairman. Thank you, gentlemen, for your excellent testimony. Let me just raise a few issues.

Professor Streff, you pointed out or suggested in your comments that the location of data centers here *versus* overseas tend to build a level of protection because of our laws, but it raises a larger question of the international application of any of the standards we develop and a related question of we could have a very sophisticated national regime of protection, but if it is an international economy, the back doors could be elsewhere. So I wonder if you could comment and then ask your colleagues on the panel to comment on that.

Mr. STREFF. Sure. Thank you. I like the Administration's proposal of identifying and prioritizing critical infrastructure protection, critical infrastructure that we depend upon, and then, based on that, making decisions regarding protection. Certainly, offshoring data centers and not controlling physical security, the

differences in the different laws, privacy and security laws of different nations, you know, weave the fabric and make it even more difficult. So I know that the proposal addresses the data centers here in the U.S. and being careful about offshoring that kind of activity, and the National Center for the Protection of the Financial Infrastructure certainly agrees.

Senator REED. Let me just add another sort of level. Is it feasible, practical, to insist that we have jurisdiction—if it is an American entity that has set up the center overseas, that we have jurisdiction and that we can at least inspect, investigate, and correct? You might want to comment, and then I will turn it over to the rest of the panel.

Mr. STREFF. You know, I guess from a legal perspective, I will leave that to our Georgetown colleague, but certainly from our perspective, what we are seeing is there are certainly ways that you can audit those kinds of organizations, just like they do here in the U.S. in terms of, like, service providers and data aggregators and things like that. In terms of the legal aspects, I guess I would leave it to my colleague.

Senator REED. Mr. Pratt, and then we will go right down and we will definitely get the Georgetown connection.

Mr. PRATT. Today, if we look at Title 5 of GLB today as an example of a data security regime, it applies to the practices of that financial institution, our members included, wherever we may locate that data center. I know even the CDIA has stood up several different data centers, and even here in the U.S., we look at different power grids. We try to separate the back-up system from the primary with power grid differences. We look at plate tectonics to see if we have them on the same earthquake fault line or not, these sorts of things.

And candidly, whether it is overseas or whether it is here in the U.S., the U.S. law applies to the U.S. business. And, in fact, all of those requirements that the Professor just outlined, you know, the physical security, the employee training, the technology that has to be deployed, all the requirements of the Title 5 apply and the examination powers and the bank agency powers and the Federal Trade Commission powers apply.

So I am not sure whether it is in the West Coast or the East Coast or just off of one of those two coasts makes a difference in terms of data centers. The key is to make sure the data centers are managed properly and those risks are assessed and accounted for.

Senator REED. Mr. Williams, shortcomings?

Mr. WILLIAMS. I wish Mr. Pratt would say something I could disagree with, but I cannot disagree with that. Our financial institutions are already accountable for what happens at their direction, whether it is at a service provider or in their own subsidiaries, whether it is within the U.S. borders or outside the U.S. borders. They are held accountable by their regulators, and on the jurisdiction question, they should be held accountable by this Committee.

We believe that the same logic should apply outside of financial services. So if this proposal or some proposals like it begin to address cybersecurity in the ecosystem, all players should be accountable for what happens at their direction inside or outside the U.S. borders, inside or outside of their legal ownership.

One of the stipulations in the cybersecurity proposal offered by the Administration takes State data centers and says that there may be no restrictions in the borders among the U.S. States. We believe that because we need this ecosystem-level protection, that should be extended even beyond the U.S. outside to international operations.

Senator REED. Professor, but I just want to throw in another issue here, too, not to go into really complicated things, but you refer in your testimony to the effectiveness of State laws, and there was a colloquy back and forth with the Chairman about the need for a national standard. I have seen sort of this debate in many different contexts, and a national standard is terrific if it is tough and strong and reaches all the players. It is less effective—and we saw this particularly in the case of predatory lending—when the national standard is rather low and State standards, much more effective, are legally sort of avoided under Federal regulatory preemption. So you might want to comment on that in this context, too.

Mr. ROTENBERG. Senator, these are the two critical issues. With respect to preemption, I certainly appreciate the position of the business groups. I am sure that a national standard would be easier to administer, but I think it is very important to look at the practical effect when a low national standard removes higher State safeguards. And even the States themselves have learned that they do not always get it right the first time. That very good California breach notification law covered only financial institutions. They had to come back and update the law to deal with medical record information when they realized they would have a problem there. So that is another reason I would urge caution on a Federal standard that ties the hands of the States.

Now, the other question you raise, Senator, is also key in this area. We are in a global economy with global businesses. Particularly with the Internet, people are purchasing products all around the world and a lot of customer data moves around the world, particularly now that we have cloud computing services that are offered in many different jurisdictions.

We have actually worked with the Administration to urge the development of a comprehensive framework for privacy protection, and there is interest. In fact, part of the White House cybersecurity strategy talks about the need to strengthen privacy safeguards for commercial data flows, particularly between the United States and Europe. We hope they will go further for many of the reasons that you have outlined. The Europeans are also concerned about what happens to their financial data. There is a need to establish there a common framework with clear legal protections. And I think what you are reading now about the data breaches, of course, it is not just customers in the U.S., it is people all around the world.

Senator REED. Agent Martinez.

Mr. MARTINEZ. Senator Reed, from a law enforcement perspective, storing data overseas does pose a challenge. For example, look at it from the point of view of a crime scene. Now we have a crime scene, and instead of just being located within the United States, it is located in different parts of the world, posing challenges to the type of legal process that we could utilize to obtain that informa-

tion. Is there legal process in that country where I seek that information that is pertinent to my case? How long will it take me to obtain that information? I now might have to do what is referred to as a Mutual Legal Assistance Treaty Request to that specific country.

The violation that I am investigating the criminal for, is that a covered violation within that country's legislative process? We have been encouraging our international partners to join in the Budapest Crime Convention because it talks about establishing cyber crime legislation like this throughout different countries around the world. But it does pose challenges to us and it makes it much more difficult and it takes more time for us to obtain that information.

There are extraterritorial violations, for example, even in the area of identity thefts. Credit card fraud has an extraterritorial section to it where we can use that part of the statute to prosecute people who commit credit card fraud using U.S. accounts domestically. But I think it is a challenge that will be tested here sooner rather than later.

Senator REED. Thank you, gentlemen. Thank you, Mr. Chairman.

Chairman JOHNSON. Senator Menendez.

Senator MENENDEZ. Thank you, Mr. Chairman. Just to show you how timely these issues are, Mr. Chairman, as we are speaking, a widespread phishing campaign is being targeted on Senate staff with a false IRS statement that if you open up downloads a malicious link. So this is a constant challenge, and including the United States is not immune from it.

Mr. Williams, let me ask you, I look at the number of attacks that have taken place, particularly in the last 6 years. There have been 288 publicly disclosed breaches at financial service companies that exposed at least 83 million customer records. And I am wondering, what is your view from the industry perspective as to what is the fiduciary duty here by these institutions to notify their customers in a timely and efficient fashion?

Mr. WILLIAMS. There is no doubt in my mind that institutions have a fiduciary responsibility, they have a commercial responsibility, they have compliance responsibilities, and that they take all of those very, very seriously. We do an enormous amount of work with member institutions on preventing breaches and ensuring that when they do occur, they are absolutely responded to as quickly and as completely as possible.

Senator MENENDEZ. Do you think a month to notify customers is an appropriate time frame?

Mr. WILLIAMS. I think that as soon as an institution understands what has occurred, they have an obligation to notify their regulators under regulatory rules and they have a fiduciary and a business responsibility to notify customers if there is any way that those customers can begin to take action to protect themselves.

Senator MENENDEZ. All right. I appreciate that answer, because from what I can perceive of Citi's response, that was not the case, as is evident by just the personal story I related before. It took a lot more time, and that does not allow people to protect themselves.

Agent Martinez, is not information and notification one of the essential elements for someone to try to limit the scope of the damage done to them once they know they can act?

Mr. MARTINEZ. Yes, sir. I believe the Administration proposal calls for a certain time frame by when victims have to be notified. I think it is also important to realize that, when it comes to law enforcement's investigations, a more clear, concise, and exact set of events for the financial institution to know what exactly has happened and to be able to relay that to the law enforcement organizations in an efficient and effective way helps us significantly, instead of getting dribs and drabs of information.

So although I do not think—I agree with you that notification needs to be made as soon as possible, we would like a clear and concise picture of what they have, and I think the Administration's proposals on data breach lay out specific time lines that we think is enough time for institutions to have that information.

Senator MENENDEZ. Well, I look at NASDAQ, World Bank, Citi, just to mention some, and I wonder whether there is anyone on the panel who wants to give an opinion as to whether or not financial institutions are seriously taking the challenge before them and making the appropriate investments in trying to protect against cybersecurity attacks.

Mr. WILLIAMS. I can assure you, they absolutely are taking it seriously. They are investing tens of billions of dollars at an institutional level and at an industry level. I cannot promise you that there will never be another breach in financial services, but I can tell you that we constantly improve our ability to repel these attacks and we constantly improve our ability to protect against inconvenience and any financial loss on the part of customers or institutions. We are getting better and better at this every single day.

Senator MENENDEZ. Mr. Rotenberg.

Mr. ROTENBERG. Senator, I wish I could agree with my colleague, but I think the experience of consumers today is actually very different. It may be the case that financial institutions are spending a lot of money to safeguard this data, but what consumers are seeing are more and more breach notifications, more and more warnings that their credit card information is in the hands of others, more and more recommendations that they may need to change their bank account numbers.

We have a problem, and this problem is getting worse. I do not mean to suggest that passing legislation is going to solve it. I think it will help make clearer the scope of the problem and make possible some other approaches. But I do not think we can overstate quite how serious today the problem of data breach is in the United States.

Senator MENENDEZ. Mr. Pratt, did I see you wanting to comment?

Mr. PRATT. I would just—I would add, first of all, I think some of the examples you have given are very helpful for all of us because different breaches have occurred in different ways. Where there is a phishing attack or where you are fooled into clicking on an executable file that then scans your hard drive, this is different than a cyber attack against a Web site.

Our own members, for example, have had to develop Web sites for expatriates to access certain data here in the U.S. and that entire data network is separate from the U.S.-based system, which is a significant investment to create entire duplicate systems, and that is all for that very reason of trying to protect data and to ensure that the higher risk that we have from foreign access is balanced against the domestic risk.

So I would agree with Mr. Williams. There are enormous investments. It is a constant moving target, as you know. You are very experienced with this. You have the bills in place to look at this. We are constantly sharing with information sharing and analysis centers to try to understand what other financial institutions have experienced in order to learn from that, in order to better our own systems, in order to take the next step to anticipate what the risk is. So it is a moving target challenge. It is a challenge for small retailers who may lose credit card account numbers, not because the bank has failed but because the retailer may have failed in that case to protect the information at the retail level. There are some older breach examples where some retailer systems were storing data that they should not have been storing based on guidance that was out there.

We have to unpack all of these fact patterns. We have to learn from these fact patterns. We have to make better decisions going forward. We believe that we are.

Senator MENENDEZ. Well, I thank you, and let me, Mr. Chairman, let me just close by saying, I hope some of you will look at the Cybersecurity Enhancement Act that we are offering. We think it is an opportunity to do research and development, bring the three entities, the National Science Foundation, Department of Homeland Security, and Department of Defense leading in the Federal perspective, and then seek to commercialize that so that we can have institutions look at it.

But the one thing that I am still alarmed at—I know this is a moving target, but the one thing I am still alarmed at is timely notice to customers. I think it is essential for a good business relationship, certainly it is essential for the consumer, and I would like to see an industry response to that. But in the absence of it, there will be some of us who will consider legislative responses.

Thank you, Mr. Chairman.

Chairman JOHNSON. Senator Merkley.

Senator MERKLEY. Thank you, Mr. Chair.

I think I am going to follow up on this consumer notification. More and more citizens have had the experience of receiving a letter saying that there was a breach of data at our institution and your records may have been among the records lost. This certainly happened with my wife through her place of employment, and some of these breaches have been through Web sites being hacked, but others are as simple as information left on laptops that were stolen out of cars and things of this nature, and it is not always clear in whose hands this information is going to end up in.

Oregon has adopted some provisions related to this, but I just wondered, and maybe, Mr. Rotenberg, you would like to kick this off, are there States that have a particularly successful model that should recommend itself to our examination here?

Mr. ROTENBERG. Well, Senator, California tends to be on the front lines of these issues, and I think their efforts not only in establishing early on a breach notification requirement and then updating it has been successful, other States, as well. But as I spoke with some of the consumer experts prior to this hearing, they made additional recommendations. It would be helpful, example, I think, when a person receives one of these notifications to actually be told by the institution what the institution has done to correct the problem. If we think about it for a moment, when someone has had a problem that affects us, we want to be assured that it will not be repeated in the future. So I think actually saying explicitly what the institution is doing to ensure that the problem will not be repeated would be a good step.

Also, with respect to credit card information, you know, the current system in the U.S. allows people to get access to the credit card information of others unless they have explicitly chosen to freeze the access. You might think of this as the difference between opting out *versus* opting in. A number of States are moving toward these freezes on credit card information which gives individuals the ability to say if, for example, they are shopping for a car, OK, now you can look at my credit record information, but otherwise, I do not want other people to be looking at our credit record information, and I think this is another innovative approach that would be worth looking at.

Senator MERKLEY. So some of the things that were discussed in Oregon, and I would have to go back and see what all was adopted, but it was also kind of a protocol for responding to customers whose data has been breached, kind of providing them with the tools that they need, the access that they need in order to be able to monitor. OK, credit card information was stolen, but what help can they get in fast detection of someone misusing that information? Is that part of the California model?

Mr. ROTENBERG. Yes, and I should mention, also, the Federal Trade Commission has put together very good resources that are available on the FTC Web site to help consumers who have been the victims of identity theft. But I have to say, I think, also, people are just becoming very frustrated. It takes time to walk through these steps. There is no necessary assurance that if you have done everything you are supposed to do, you might still not find an improper charge somewhere down the line.

And so I think we actually need to be thinking more long-term about how to minimize the risk when the breach occurs, which is the reason why in my testimony I talked in some detail about this concept of data minimization. For example, Social Security numbers. I mean, for a long time, it has been understood that Social Security numbers should not be widely available because they are too frequently used as passwords. Yet you have the case today that health club members are required to provide Social Security numbers to join the health club, which seems to create an unnecessary risk.

Mr. STREFF. Senator, if I could comment, as well, you know, I think if you—most of the State laws exempt financial institutions. And if you really take a look at when this happens, there is a tremendous cost, like, to the small- and medium-sized financial insti-

tution. The Ponemon Institute publishes that it is about $202 a data record that is breached. So if you are a small financial institution, you have got a thousand customers, you can do the math. That is fairly significant. And I am not minimizing this.

I would encourage the Administration, as they are looking at this, it seems to me that this gets minimized all the time, so I am glad to hear you folks talking about this. The Epsilon attack, to me, is a good example of how this gets minimalized. If you read the press clippings on that one, thankfully, all that was stolen were email addresses and names. Now, does that require data breach notification, because it is not Social Security numbers, it is not financial account numbers. That is a serious issue when email addresses with names are disclosed, because that sets up phishing attacks and that sets up all other kinds of attacks. So I would encourage the Administration to think that through as they are drafting policy.

Senator MERKLEY. So, Professor, to go back to your point, you said the cost to a small business of addressing the loss of data, the average is $200 a customer?

Mr. STREFF. Two-hundred-and-two dollars, sir. If you really take a look at do you cut up the cards, do you issue new account numbers, do you provide fraud detection services, you know, all those kinds of things, the Ponemon Institute has "mathed" [phonetic] that out to $202 a data record.

Senator MERKLEY. I am over my time, but I will ask more questions if we continue this.

Chairman JOHNSON. Please proceed with your questions.

Senator MERKLEY. Thank you very much, Mr. Chair.

I want to shift a little bit to the issue of liability. Recent courts have come down on both sides of the issue of bank liability for data theft, some saying banks are not liable if they meet the minimum regulatory standard, others finding higher duties to customers. So I would just open this up to any of you who would like to comment. How should liability be configured to maximize cybersecurity protections while minimizing litigation uncertainty?

Mr. WILLIAMS. Many of our member institutions see their responsibilities to customers not in terms of legal liability but in terms of the relationship that they have built with these people. I think whether, for example, they are required to or not, they do everything in their power to minimize, often to zero, generally to zero, the risk of customers, especially at the retail level, in breaches or in other cybersecurity incidents. There has been some talk about whether that protection that retail customers enjoy, sometimes voluntarily, sometimes under regulation, should be extended to commercial customers, some of whom look and act a little bit like retail because they are smaller or because of the way that they operate.

We would be reluctant, I think, to see that put into rule or statute. There is this bright line between individuals and institutional clients, and there are already under the banking regulations ways that those two entities or classifications of entities are treated differently. We do what we can to ensure that individuals are protected and to ensure that their financial losses are managed to zero, and we do what we can on the institutional side, but the pro-

tections are a little different and the liability scheme may also be appropriately different.

Senator MERKLEY. Mr. Williams, how do you, in general, how do people who have small home businesses, if you will, the small businessman who is a Chapter S Corporation, they are simply—their money comes through their personal taxes—are they viewed as an institution in that framework or as an individual?

Mr. WILLIAMS. We tend in most institutions to think of it based on the type of account that they have. So if they have a personal account, they are treated as individuals. If they have a business account, then we treat them under the law as business customers.

Senator MERKLEY. OK. Thank you.

Anyone else on this liability, kind of the need to have some certainty over litigation exposure versus working to make sure that it is made right when there is a breach?

Mr. ROTENBERG. Well, Senator, I think the economists would say that the liability should be assigned to the least cost avoider, which is to say the institution that is in the best position to minimize the risk. And this is an important principle, because when you think about the customer who gives over the information to the financial institution, they actually at that moment have lost the ability to control the subsequent use of the data they have provided. This is, as Mr. Menendez says, this creates the fiduciary obligation that the financial institution now has, and that is one of the reasons that I think it is so important that that risk be shifted from the individual, because they are simply not in a position to reduce subsequent risk of misuse.

Mr. PRATT. Senator, I would only suggest that—in fact, we have this in our written testimony—that one of the successes of the data safeguards rules is that they are administratively enforced. That does not mean that they are passively administratively enforced. That is an aggressive program, as we discussed before, examination processes and the Federal Trade Commission uses CID processes and so on to do that. In the case of Fair Credit Reporting Act, State Attorneys General also have the ability to enforce the law.

What we would like to avoid, however, is almost a division of the country circuit by circuit. There are other places in our membership where we have companies that actually have to comply with certain requirements because circuit by circuit decisions have actually divided the country and it makes data security less effectively administered, or some other kind of compliance program less effectively administered.

So our argument is not for ineffective administrative powers, but just simply to ensure that if there is an administrative power, that it is uniform and applied across the country, and you just simply cannot accomplish that if you are going to have, for example, a private right of action that would begin to divide the country into circuits. So we need that uniformity in order to be successful. We want to be successful. We want that data protected. And we also want to notify consumers where data has been lost or stolen and we know that we have a responsibility to make sure that consumer is made whole.

Mr. STREFF. You know, I think it is fairly risky business to be Reg E-ing corporate accounts. This is my perspective. You know, in

my research, as I mentioned, seven out of ten small businesses lack the basic security controls of access control or a firewall or antivirus, basic stuff that we all should have on our home environments and certainly in our business environments. Because of those deficiencies, corporate account fraud is occurring. The keys are laying there on the small business desk and the crooks are picking them up and simply logging into the bank and doing nefarious activity. So I think we want the accountability at the corporate account at the small business, and shifting that to the bank, I am not sure if that is where the real issue lies.

Senator MERKLEY. So do you see a difference between fraud that stems from people leaving the keys on the home desk versus fraud that occurs because of a central data base in an institution is hacked or records are copied onto a personal computer and stolen or something of that nature?

Mr. STREFF. I certainly do, and I think the courts are trying to sort of figure out where those lines are. The EMI America case that just was announced, the decision last week, where it is trying to draw some of those lines about the definition of what is commercially reasonable security, you know, I think that that is what the courts are trying to figure out, and without further policy on that, I think the courts will struggle to interpret that.

Senator MERKLEY. I want to shift gears. I have one more question if there is time for it.

Chairman JOHNSON. Yes.

Senator MERKLEY. This is related, although it is a bit afield from the immediate conversation, but this is related to issues that derive from changes in technology and mobile banking. One of the things we have started to see more about, or at least I have started to see more about, is the issue of remotely created checks, or RCCs. The States Attorneys General and the Federal Reserve have identified a high incidence of fraud, and it is kind of interesting that these remotely created checks only require verbal authorization, which is undocumented in the process. So that immediately looks like a weak link in the system. My understanding is payday loan companies tend to be a major user of this, but also fraudsters are seeing this as a weak link.

And so there has not been a lot of response from OCC or the Federal Reserve, and I just wanted to get, if any of you have any insights on this issue and think it is fine the way it is or do we need to modify the system of remotely created checks.

Mr. WILLIAMS. I can tell you that many institutions are looking at which of their clients they are comfortable with and finding ways to monitor the behavior of those clients. So if there are some that are processing remotely deposited checks or remotely created checks and they see a pattern of many of those checks being returned, our institutions typically will shut those customers down and will file suspicious activity reports so that they cannot open accounts elsewhere.

Senator MERKLEY. Do they still serve an important enough role in the system that they should still be allowed, or do we have—we have other options and strategies now to do those sort of electronic transactions. Are they kind of an anachronism that we could just as well do without?

Mr. WILLIAMS. They are an interesting bridge between old mechanisms, like paper checks, and new ones, like ACH entries.

Senator MERKLEY. Yes.

Mr. WILLIAMS. ——and it may well be that we can evolve past them and at some point they will no longer serve a purpose.

Senator MERKLEY. Anyone else? Any other thoughts on this?

[No response.]

Senator MERKLEY. OK. Well, thank you all very much for your testimony. This is an area, certainly, of importance to our businesses, our financial institutions, and our citizens.

Thank you, Mr. Chair.

Chairman JOHNSON. I want to thank the witnesses for the testimony on this important issue. I think that today's hearing yielded some good information for us to review as we consider this issue going forward. Thanks again to my colleagues and our panelists who have been here today.

This hearing is adjourned.

[Whereupon, at 11:14 a.m., the hearing was adjourned.]

[Prepared statements and additional material supplied for the record follow:]

PREPARED STATEMENT OF CHAIRMAN TIM JOHNSON

The Banking Committee meets today to hear testimony about data protection and cybersecurity issues in the financial sector.

Over the past 12 years, the Committee has enacted several pieces of legislation to protect consumer data held by financial institutions. Federal financial regulators under the Committee's jurisdiction have issued extensive rules and guidance on data practices that require the institutions they regulate to keep data secure, notify customers and regulators when breaches occur, authenticate customers, and notify customers about how their sensitive information may be used.

Recent high-profile data breaches at major institutions within the financial sector and elsewhere underscore the importance of cybersecurity for the American economy. Breaches are disruptive and raise the potential for financial fraud, identity theft and, potentially, severe threats to our national economic security. This is an important issue that deserves the Committee's careful attention and continued oversight. Today, I invite the witnesses to share their views in three areas:

- The current regulation of data practices affecting financial institutions and their customers;
- The current state of data privacy protection, data breaches and cybersecurity in the financial sector; and
- How legislative proposals, such as the Administration's cybersecurity bill, would affect financial institutions and would interact with existing regulation

I look forward to the testimony of our witnesses, and to the question and answer period.

PREPARED STATEMENT OF KEVIN F. STREFF

ASSOCIATE PROFESSOR OF INFORMATION ASSURANCE, DAKOTA STATE UNIVERSITY
INFORMATION ASSURANCE CENTER

JUNE 21, 2011

Introduction

Chairman Johnson, Ranking Member Shelby, and Members of the Senate Committee on Banking, Housing, and Urban Affairs, I am pleased to appear before you today on behalf of the National Center for the Protection of the Financial Infrastructure (NCPFI) at Dakota State University to share our views on the current state of data/cybersecurity as relating to small- and medium-sized financial institutions and what they do well/or not so well. These comments will be made within the context of the President's recent proposal regarding The Comprehensive National Cybersecurity Initiative (CNCI) which is vital to increase America's detection, planning, and response capabilities as it relates to attacks on our Nation's critical electronic infrastructure.

My name is Dr. Kevin Streff and I am Director of NCPFI from Madison, South Dakota. The NCPFI's mission is to "advance the security and safety of the Nation's financial infrastructure through research, education and outreach." Started in 2009, the NCPFI has worked with academia, the private sector and Government to bring attention to the homeland security, critical infrastructure and cyber risks associated with the electronic infrastructure which runs the financial industry. The work of NCPFI is funded by the State of South Dakota, NSF, DoD, DHS, Cheneega Logistics, and other Federal and private entities. We appreciate the invitation to appear before the Committee on this important issue, and thank the Committee for their leadership and foresight in dealing with these issues before a crisis state.

Background

Every day cyber criminals are scanning Government, academic, and industry networks for nonpublic information they can steal. Large corporations have in-house IT departments to protect their systems and customer data. Small- and medium-size financial institutions (SMFIs) and small- and medium-sized businesses (SMEs) businesses do not.

Furthermore, Presidential Decision Directive 63 deemed the financial services sector a critical cyber infrastructure which America depends upon every day; however, small- and medium-sized financial institutions are under heavy cyber attack and lack the requisite skills and resources to combat these cyber threats. Without an understanding of the risks each institution incurs and a capability to deploy solutions to mitigates these risks, it is unlikely decision makers in these SMFIs will win the battle against cyber thieves.

In this testimony, we will review the current legal and regulatory environment in which small- and medium-sized financial institutions must operate (SECTION I), discuss security and privacy experiences in the financial services sector that have impacted small- and medium-sized financial institutions (SECTION II), and discuss how the Administration's cybersecurity bill will interact with existing regulation and affect SMFIs. Some additional ideas and concerns are noted for the President to consider as it relates to the Comprehensive National Cybersecurity Initiative (SECTION III).

SECTION I. Overview of Current Data Protection Laws, Regulation, and Policy Statements in Financial Services

A. Financial Industries Modernization Act of 1999 (Gramm-Leach-Bliley)

The Gramm-Leach-Bliley Act (GLBA) 15 U.S.C. §§6801–6810 (disclosure of personal financial information), 15 U.S.C. §§6821–6827 (fraudulent access) repealed the Glass-Steagall Act of 1932, and is part of broader legislation which removes barriers to banks engaging in a wider scope of financial services. GLBA applies to financial institutions' use and disclosure of nonpublic financial information about consumers. Section 501(b) requires administrative, technical, and physical safeguards to protect covered nonpublic personal information. Federal banking agencies have published Interagency Guidelines Establishing Standards for Information Security for financial institutions subject to their jurisdiction. 66 Fed. Reg. 8616 (February 1, 2001) and 69 Fed. Reg. 77610 (December 28, 2004). The Guidelines are published by each agency in the Code of Federal Regulations, including:

- Federal Deposit Insurance Corporation, 12 C.F.R., Part 364, App. B;
- Office of the Comptroller of the Currency, 12 C.F.R., Part 30, App. B;
- Board of Governors of the Federal Reserve System, 12 C.F.R., Part 208, App. D-2 and Part 225, App. F;
- Office of Thrift Supervision, 12 C.F.R., Part 570, App. B; and
- National Credit Union Administration, 12 C.F.R., Part 748

The Federal Trade Commission has issued a final rule, Standards for Safeguarding Customer Information, 16 C.F.R. Part 314, and the Securities and Exchange Commission promulgated Regulation S-P: Privacy of Consumer Financial Information, 17 C.F.R. Part 248 for financial institutions within their respective jurisdictions.

GLBA requires financial institutions to disclose privacy notices to all customers, and provide a means for customers to opt out of the sharing of information with third parties. However, it is §6801, "Protection of Non-Public Personal Information" that contains the most sweeping provisions, by requiring each regulatory agency to:

> Establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards to:
>
> 1. Insure the security and confidentiality of customer records and information;
> 2. Protect against any anticipated threats or hazards to the security or integrity of such records; and
> 3. Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

These requirements mean that all financial institutions must develop, document and operationalize a comprehensive information security program. The administrative, technical, and physical safeguards are sweeping and expansively interpreted by Federal and State regulators to include everything from the physical security of buildings, data security at service providers, to the types of authentication used during online banking sessions. Each bank must report annually to the Board of Directors on the status of the information security program.

The Guidelines require a risk assessment designed to: "identify reasonably foreseeable internal and external threats" to customer information, assess the likelihood and potential damage of these threats, and to assess the effectiveness of a wide variety of information security controls. GLBA is significant because of the extensive requirements and regulatory oversight imposed upon the financial industry and carried out by Federal and State regulators.

The Interagency Guidelines Establishing Information Security Standards includes a provision to implement a notification program to notify customers, regulators and law enforcement officials of data breaches. The regulations promulgated to implement the response program have been codified as Supplement A to Appendix B of 12 C.F.R. Pt. 30. "[E]very financial institution should . . . develop and implement

a risk-based response program to address incidents of unauthorized access to customer information in customer information systems" regardless of whether the breach occurs in the financial institution's own computer systems or those hosted by third party service providers.

B. Bank Secrecy Act

In 1970, Congress passed the Bank Secrecy Act (BSA). BSA requires U.S. financial institutions to assist U.S. Government agencies to detect and prevent money laundering. The act specifically requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding daily aggregate amounts of $10,000, and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities. Several anti- money laundering acts, including provisions in title III of the USA PATRIOT Act, have been enacted up to the present to amend the BSA. (*See,* 31 USC 5311-5330 and 31 CFR Chapter X (formerly 31 CFR Part 103)). The documents filed by financial institutions under BSA are used by law enforcement agencies, both domestic and international to identify, detect and deter money laundering whether it is in furtherance of a criminal enterprise, terrorism, tax evasion, or other unlawful activity.

C. USA PATRIOT Act

The USA PATRIOT Act (Patriot Act), enacted by President George W. Bush in 2001, reduced restrictions on law enforcement agencies' ability to search telephone, email communications, medical, financial, and other records; eased restrictions on foreign intelligence gathering within the United States; expanded the Secretary of the Treasury's authority to regulate financial transactions. Section 314(b) of the USA PATRIOT Act permits financial institutions, upon providing notice to the U.S. Department of the Treasury, to share information with one another in order to identify and report to the Federal Government activities that may involve money laundering or terrorist activity. More specifically, the BSA authorizes the Treasury to require financial institutions to maintain records of personal financial transactions that "have a high degree of usefulness in criminal, tax and regulatory investigations and proceedings" and to report "suspicious transaction relevant to a possible violation of law or regulation." Again, because The Patriot Act deals with governmental, rather than private, intrusion into customer privacy, it is outside the scope of this discussion.

D. Identify Theft Red Flags Rule

The Identify Theft Red Flags Rule (Red Flags Rule) requires financial institutions to implement a written Identity Theft Prevention Program that is designed to detect the warning signs of identity theft in their daily operations. By identifying red flags in advance, financial institutions will be better able to identify suspicious patterns that may arise, and take steps to prevent a red flag from escalating into identity theft.

A financial institutions' Identify Theft Red Flags Program should enable the organization to:

1. Identify relevant patterns, practices, and specific forms of activity—the "red flags"—that signal possible identity theft;
2. Incorporate business practices to detect red flags;
3. Detail appropriate response to any red flags you detect to prevent and mitigate identity theft; and
4. Be updated periodically to reflect changes in risks from identity theft.

Shortly thereafter, regulatory agencies began issuing examination procedures to assist financial institutions in implementing the Identity Theft Red Flags, Address Discrepancies, and Change of Address Regulations, reflecting the requirements of Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003.

E. Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002 (SOX) was enacted to restore confidence in the integrity of the financial reporting process at publicly traded companies, influenced by high profile accounting scandals at firms such as Enron and WorldCom. However, each publically traded financial institution that is affected by the Sarbanes-Oxley Act has some level of reliance on automated information systems to process, store and transact the data that is the basis of financial reports, and SOX requires financial institutions to consider the IT security controls that are in place to promote the confidentiality, integrity, and accuracy of this data. SOX states that specific attention should be given to the controls that act to secure the corporate network, prevent unauthorized access to systems and data, and ensure data integrity

and availability in the case of a disaster or other disruption of service. Also, each system that interfaces with critical financial reporting data should have validation controls such as edit and limit checks built-in to further minimize the likelihood of data inaccuracy.

F. Payment Card Industry Standard

The Payment Card Industry Security Standards Council is an industry group formed to manage and maintain the Data Security Standard (DSS), which was created by the Council to ensure the security of payment card information. Sensitive data is involved in card transactions, including account number, cardholder name, expiration date, and PIN. The intent of the PCI DSS is to ensure that card transactions occurring across multiple private and public networks are subject to end-to-end transaction security. The payment card industry consists of Card Issuers, Card Holders, Merchants, Acquirers, and Card Associations. From the collection of card information at a point of sale, transmission through the merchant's systems to the acquiring bank's systems, then on to the card issuer, the PCI DSS requirements attempt to ensure sufficient security safeguards are in place on the card data from beginning to the end of a card transaction. Enforcement of the security requirements is done by the card associations and through a certification process of each association member. The certification process is carried out by Qualified Security Assessors (QSA), who audit systems and networks to ensure the mandatory controls are in place. Certification does not guarantee that an organization will not suffer a data breach, as several PCI-certified organizations have suffered data breach incidents.

G. Regulatory Guidance

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the Federal examination of financial institutions by the Federal financial regulatory agencies. As such, the FFIEC publishes the "Information Technology Examination Handbook", which is used by banking regulators in executing examinations of information technology and systems of financial institutions. The Handbook includes ten (10) booklets, one of which is the "Information Security Booklet", which provides a baseline against which a financial institution subject to GLBA can be evaluated. The "Information Security Booklet" attempts to provide a high level, comprehensive overview of the major types of information security controls one would necessarily expect to be operating effectively within a financial institution. The types of controls are not limited in applicability to just financial institutions, and are derived from the same principles underpinning all major information security frameworks.

Further, each regulatory agency produces further guidance for their financial institutions. For example, FDIC FIL-103-2005 Authentication in an Internet Banking Environment established single factor authentication (such as a User ID and password) as necessary but insufficient in logging users onto electronic banking systems, requiring the use of an additional factor to establish identity. This FIL involved industry investing in multifactor authentication solutions, vendors leveraging these solutions in their systems, and financial institutions operationalizing them. A second example is Corporate Credit Union Guidance Letter 2010-01 dated July 8, 2010, entitled "Confidentiality and Protection of Sensitive Data". The OCC occasionally issues security bulletins, while FRB issues Supervision and Regulation Letters (an example includes the April 4, 2011, release of SR11–7 entitled "Guidance on Model Risk Management"). The FDIC also authored the Information Technology Officer's Questionnaire, whereby an officer of the financial institution must document, attest, and sign to 71 questions in five information security categories: risk assessment, operations security and risk management, audit/independent review program, disaster recovery and business continuity management, and vendor management and service provider oversight. This questionnaire is periodically updated and released as the security/technology landscape changes.

H. Third-Party Self Regulation

Small- and medium-sized financial institutions depend heavily on hardware and software vendors for nearly all banking products. In addition, many of these vendors become service providers offering to host and manage their products for the SMFI. The service provider industry has experienced several significant data breaches affecting the financial services industry in the past several years, including ChoicePoint (163,000 data records), TJX (100 million data records), Heartland Payment Systems (130 million data records), *etc.* When companies choose to outsource data processing to a third party, they typically perform information security due diligence on the third party to understand how the data will be protected. A very

common standard for third party assurance has been the SAS 70; however, the SSAE16 standard is replacing the SAS70 and moving more to an attestation model (similar to independent financial audits). BITS, a nonprofit organization, has also attempted to standardize the assessment of third-party service providers by developing the "BITS Framework for Managing Technology Risk for Service Provider Relationships", which includes two tools to help service providers in control selection and implementation. The first tool is called Standardized Information Gathering Questionnaire (SIG), which is a template based on the ISO 27002 standard, and specifies the expected information security controls that should be in place at the service provider organization. The second tool is the Agreed Upon Procedures (AUP), which serve as testing procedures meant to validate the effectiveness of the controls specified in the SIG.

In summary, SMFIs operate in an increasingly complex regulatory environment, with community banks regulated aggressively and credit unions a little less. This regulation is necessary, but causes significant financial, resource, and other issues in SMFIs who must leverage technology to compete. Increasing regulation is likely as additional technologies are deployed and the cybersecurity stakes grow, but all increased regulation must be tempered with a SMFI's ability to stay in business and meet the needs of their customers. The majority of SMFIs are in rural locations and may be the only local funding source for a community.

SECTION II. Data Security and Privacy Issues in the Financial Sector

- Over 500 million data records have been breached since the ChoicePoint breach of 2005: 534,232,379 RECORDS BREACHED from 2,539 DATA BREACHES made public since 2005 (Source: PrivacyRights.Org).
- How many of these data records and breaches involved the financial sector? 247,808,947 RECORDS BREACHED from 386 DATA BREACHES made public since 2005 (Source: PrivacyRights.Org).

U.S. SMFIs and SMEs are important as millions of consumers depend upon community banks, credit unions, accounting firms, tax-preparation firms, investment offices, insurance agencies, and the like. When issues in the financial system exist, confidence erodes and consumers are left paralyzed wondering what to do. Similarly, as Deborah Platt Majoras Chairman of the Federal Trade Commission stated at High-Tech World, 2005, "when data breaches or an infrastructure attack occurs, customer confidence is eroded and spending is held close to the vest." The margin for error in SMEs is relatively small, and one such data breach can shut the doors on viable businesses.

Further, if terrorists would target these vulnerable SMFIs or SMEs, they would find a soft underbelly of relatively under-protected targets. A plethora of nefarious activities are then possible, including stealing and selling customer data, extorting ransoms, "owning" the computer, making these systems unavailable, *etc*. Stated directly, these activities could be enough to put a SME or SMFI out of business. The reality is that while it is nearly impossible to challenge the importance of SMEs and SMFIs in the U.S., it is equally difficult to convince security experts that either are prepared to protect their critical systems, important customer information and do their part to battle against the war on terror.

The Federal Government identified banking and finance as a critical infrastructure that requires protection, yet most of the attention is paid to the large financial institutions. SMFIs and SMEs store and transmit much nonpublic data, with limited resources to fend off a well-equipped, well-funded enemy. A recent survey of bank executives called out this very fact. When asked what their top technology concern was over the next 2 years, risk management and compliance topped the list. A black market drives insiders and hackers to steal information because of its value. An article in *Information Week* highlighted the problem: "More electronic records were exposed in 2009 than in the previous 4 years combined and most of those breaches—nine out of ten—could be easily avoided with basic preventative controls consistently applied." SMFIs and SMEs have a wealth of nonpublic, sensitive data that cyber thieves are targeting with increasing regularity.

Cybersecurity is a broad and pervasive issue leading to at least two national issues: critical information protection and identify theft. Critical information protection is guarding our electronic infrastructures as an issue of national security. Incidents are classified, but it is well established that China and others are interested in technology disruptions that affect the United States' ability to conduct commerce. President Obama is on record stating that the United States is not prepared for CIP and despite national budget pressures is creating a division within the national Government (Cyber Command) to begin focusing on this new national issue.

Identity theft is the fastest growing crime in America and the risks of not protecting such information can be catastrophic to SMEs in communities. When identities of good U.S. citizens are stolen by cyber criminals, the good citizen can be humiliated, lack good credit, and spend significant time and money in an attempt to partially restore their good name. Information risk management is the first step in resolving the broad and pervasive issues of CIP and Identity Theft. Public Law 111-24 was signed by the President establishing a Small Business Information Security Task Force to look into the issue. The Ponemon Institute, an independent research firm which conducts research on privacy, data protection, and information security policy, calculates in 2010 businesses paid an average of $202 per compromised record (Ponemon Institute). This equates to $101,000 for a SME with 500 customer records. SMEs who cannot securely manage customer data from identity theft face either closure or acquisition by larger metropolitan-based organizations that have in-house IT security.

"Cyber crime is having enormous real consequences, which holds the potential to cripple businesses and services," says Steven Chabinsky, deputy assistant director of the FBI's Cyber Division. He continues, "Cybersecurity is not a nice thing to have for American businesses, it is critical to their survival." Cyber criminals began by hacking phone systems and Government networks, and expanded their operations to penetrate large organizations over the past 10 years. Today, cyber criminals are expanding again, this time to target and thieve small- and medium-sized businesses. This issue is magnified in America where there is very limited information security expertise, offering unprotected businesses as easy targets for organized cyber criminals with financial motivation.

Electronic Crimes in Commercial Banking With Small- and Medium-Sized Financial Institutions

Organized cyber gangs are increasingly preying on small- and medium-sized companies in the U.S., setting off a multimillion-dollar online crime wave and grave concerns that critical infrastructure Government and business depends upon each day may become compromised. It appears there are three contributing reasons they are growing so fast: (1) Low threat of arrest in these "safe havens", (2) High payout for the crime, and (3) Victim sharing data on these attacks has been minimal. The attacks are amazingly simple and the amount of money taken, information stolen, or infrastructure compromised is concerning. SMEs do not know how to protect themselves. In some cases where credit card theft has occurred, they have had to shut down because they lost the ability to process credit cards. Small businesses are being affected greatly by poor security practices. It is not a risk issue, but rather an issue of survival.

Cyber criminals view SMEs as easy targets without the resources or knowledge to fend them off or prosecute them if caught. Consequently, cyber criminals are turning their attention to perceived easy targets in America. Identity thieves can cost SMFIs and SMEs their basic ability to stay in business (*i.e.,* financial losses, bad publicity of a data breach, significant costs of recovering from a data breach, inability to process credit cards, *etc.*). Even if there were no measurable damages to customers, the notification costs alone can put the SME out of business. One-third of companies said that a significant security breach could put their company out of business. *Information Week* reports data breaches cost an average of $202 per record breached, with $139 of this cost attributable to lost businesses as a result of the breach. Many SMEs are having a difficult time in this recession, and even the smallest of distractions can be devastating. SMFIs, too, are struggling with increased assessment fees, limited deposits, limited fee-based products, and overwhelming compliance expenses, which is spurring closures and consolidation in the industry.

While SMFIs have struggled to keep pace with hackers, the SMEs have clearly fallen short. In a study I completed of SMEs, 7 out of 10 SMEs lack at least one basic security control, such as a firewall, antivirus software, strong passwords, or basic security awareness for staff. Many SMEs simply lack the basic security most of us expect on our home PCs. As evidence, I provide a statistic. I am founder of Secure Banking Solutions, LLC, a security/privacy firm focused on information security and compliance for SMFIs. As such, SBS is regularly hired to conduct penetration tests on SMFIs where SBS security personnel run (after authorization) hacking tools to see if they can break into the bank's network and systems. SBS is effective in 27 percent of SMFIs (meaning that SBS personnel were able to gain access to information and systems they were not authorized for). To contrast, SBS is effective in 98 percent of SME penetration tests. The question is "why?" and the answer is simple: SMFIs are regulated to a certain level of security that is far superior to a SME. Most anyone can download hacking tools from the Internet, point them at a

SME, and gain unauthorized access, zombie the machine, steal data, or disrupt the environment.

Traditionally, most SMEs have viewed security as a problem faced solely by large organizations, Government agencies, or online intensive operations as large organizations possess large, prolific information targets and are generally more regulated than SMEs. However, cyber criminals are finding easy targets in SMEs that have limited security. The financial gain for cyber thieves targeting SMEs is obviously less than that of large organizations, but they can be hacked in significantly less time with little to no effort. Tools to conduct these attacks on SMEs are freely downloadable from the Internet.

Howard Schmidt, the White House Cybersecurity Coordinator, recently stated: "Around 85 percent of cyber attacks are now targeting small businesses." (Source: Howard Schmidt, White House.)

SMEs are targeted as they are easy prey and do not have the expertise to ward off attacks. Generally, SMEs with less than $10 million in revenue will be a big market over the last 18 months. Most small businesses (86 percent) do not have staff dedicated to IT security and only 28 percent have an Internet security policy, on which only 35 percent train employees.

The FBI recently issued an alert to all SMFIs and SMEs of this issue. These attacks are working because of a lack of security controls at the SME whereby fraudulent transactions are directly taken out of commercial customer's bank accounts.

> The Ponemon Institute reported in 2010 that 58 percent of small businesses had a security loss due to online banking fraud, and nearly one third of these small businesses experienced a loss of more than $5,000.

At a basic level, the attacker compromises the SME network due to a lack of basic security controls, and proceeds to install malware to steal login credentials. After receiving the login credentials (User ID and password), the hacker simply logs onto the SMFI network, escalates privileges as necessary, and steals data or money. Figure 1 outlines a typical corporate account take-over attack.

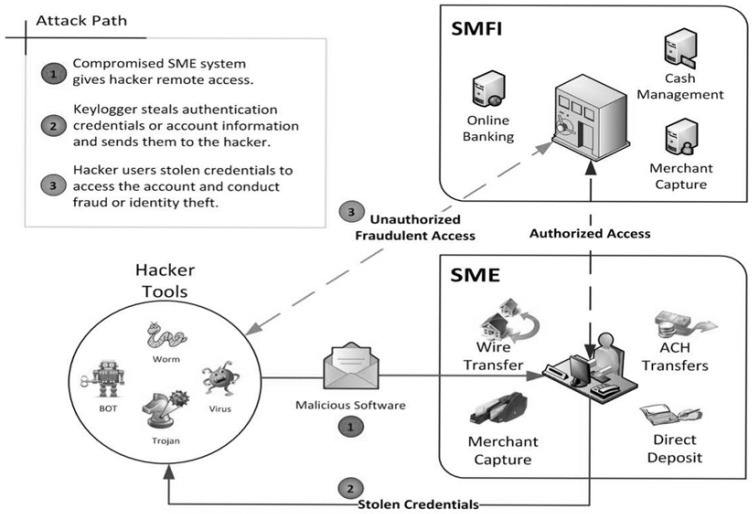

Figure 1 – Anatomy of a Corporate Account Takeover Attack

SMFIs today lack an ability to understand which businesses represent risk to these new-wave attacks. SMEs are the target of these attacks and must understand how to prevent them from occurring.

The current generation of banking products work because of technology, including remote deposit capture, Internet banking, mobile banking, item imaging, and online account origination. However, *USA Today* quoted Amrit Williams, a chief technology officer, "Any organization that cannot survive a sudden five- or six-figure loss should

consider shunning Internet banking altogether." Banking security analyst at Gartner, Avivah Litan, tells acquaintances that run small businesses to switch from commercial online accounts to an individual consumer account to take advantage of consumer-protection laws under Regulation E, because 57 percent of the time SMEs are stuck paying some or 100 percent of the bill. Regulation E protection does not exist for corporate accounts; consequently, SMEs have no legal protection if commercial account fraud occurs. Unlike individual accounts that protect individual consumers to a maximum exposure of $50 if fraud occurs, corporate accounts have no such protection. The SME can sue or go to the media, but these approaches likely do not get the money back and drains even more resources from SME which are typically resource challenged.

New fees levied by financial institutions on paper-based banking products are likely to push more small businesses into banking online, whether or not they are aware of and prepared for the types of sophisticated cyber attacks that have cost organizations tens of millions of dollars in recent months. Gartner analysts say banks should not be pushing more businesses into online banking without adequately informing them of the risks. The reality is that the perfect small-business storm is occurring: heaving attacks are already beginning and significantly more technology will be deployed by SMFIs over the next 5 years, creating a fertile cyber ground for terrorists to create problems.

The 2011 Business Banking Trust Study provides insights from the SME perspective on the pervasiveness of fraud, the state of security at banks and businesses, and the impact fraud has on businesses' relationships with their banks. The 2011 study found:

1. Fifty-six percent of businesses reported experiencing payments fraud or attempted payments fraud in the last 12 months;
2. In 78 percent of fraud cases, banks failed to catch fraud involving the illegal transfer of funds or other nefarious practices such as information identity theft; and
3. Thirty-eight percent of respondents said they access their company's banking accounts from mobile devices including smart phones and tablet PCs like the iPad, compared to only 23 percent in 2010.

The survey data reveals that despite a year of increased public attention to the impact that corporate account takeover has had on businesses and banks, the industry has barely moved the needle in addressing the problem.

The National Cyber Security Alliance has conducted a new 2011 National Small Business Security Study with Visa Inc. to analyze small business' cybersecurity practices and attitudes. Results include:

- Only 43 percent of small- and medium-sized businesses have a plan in place to respond to the loss of customer data, such as credit or debit card information or personal identifying data.
- Forty-seven percent of employees at SMEs report receiving no security training.
- Fifty-three percent of all small business owners believe the high cost in time and money to fully secure their business is not justified by the threat.
- Fifty-seven percent are NOT confident that their business is protected against cyber thieves.

In summary, there is little doubt that the financial services sector is under attack for identity theft and infrastructure corruption motives. There is also little double that the small- and medium-sized businesses and financial institutions are coming in the cross-hairs of cyber criminals. The number and significance of data breaches and attacks is significant, and only a comprehensive approach that looks at all infrastructure holistically (from Government, academia, and industry) can ward off these terrorists.

SECTION III. Analysis of Administration's Cybersecurity Bill on the Financial Industry, With Particular Attention to Small- and Medium-Sized Financial Institutions

This section will summarize the state of cybersecurity protection and compliance in both SMFIs and SMEs and discuss the Administration's Cybersecurity Bill and its impact on SMFIs.

1. Technology, Cybersecurity, and Compliance Challenges Are Outpacing the Capabilities of SMFIs and SMEs.

Technology is advancing faster than SMFIs' ability to respond with appropriate mitigating security controls. For example, the use of cell phone cameras to take a

picture of a check as the basis for making an electronic deposit into an account, or P2P, B2B, or B2P transactions by cell phone create security exposures for which there are inadequate controls to prevent fraud. Fortunately, most SMFIs are not first adopters of new technology, but rather prefer to wait until the systems become more seasoned before embracing newer technologies. Moreover, the timeline between introduction, implementation and adoption of new technology by consumers continues to shrink. Just 10 years ago, data processing was the buzz where computers were essentially back-off equipment designed to promote efficiency in the financial institution. Today, technology is front-line differentiators for banks, with customers demanding to use mobile technologies and social media to conduct banking commerce. The risk profile 10 years ago included someone breaking into the bank's computer to get customer records, while the risk profile today is someone breaking into cell phones, laptops, mobile devices, social media sites, merchants who deposit checks via imaging systems, service providers who host critical banking applications, Web sites which validate flood plains or credit bureau information, *etc.* This list goes on and on regarding the technologies typical in a SMFI. The next generation of technologies will exponentially increase the risk profile because information and infrastructure will be further distributed, and not partitioned off by the walls of the bank. With the increase in outsourcing and the mounting risks of offshoring, requiring data centers to be located in the U.S. seems consistent with the goal of increasing our cybersecurity posture. Banks leverage Brinks trucks to secure the delivery of cash to their bank. The financial industry needs to devise "cyber Brinks trucks" to perform the same role in cyberspace.

The attack target at SMFIs is typically individual accounts and small- and medium-sized business accounts (*i.e.,* corporate accounts). For the most part, cyber crooks have used malicious software to infect those computers because the controls at small- and medium-sized businesses (SMEs) are nonexistent or rudimentary at best—certainly not nearly as in-depth as even the smallest financial institutions. The PCI standards are clearly inadequate, and for the most part based on voluntary compliance and self-audit. Today, the best mitigation strategy seems to be to educate individuals and SMEs to the risks and controls that are essential to minimize the potential for major cyber loss or disruption. Moreover, we do not think it is appropriate or reasonable to shift the burden of loss from the person or organization that had inadequate controls in place to detect and deter cyber hacking attacks, to the financial institutions that process the withdrawals by the crooks, generally through ACH debits. The recent *Experimental Metal Incorporated (EMI) vs. Comerica Bank* decision is concerning to the small- and medium-sized financial sector as it appears to increase SMFI responsibilities to information risk management of corporate accounts (even if the security attack occurred at the SME). Automated systems are necessary that help individuals and SMEs identify risks, controls, and mitigation strategies. It would appear that SMFIs, which already conduct a bank IT risk assessment and a third party vendor assessment, will need to put in place a corporate account risk management program very shortly.

The mounting compliance drivers are beginning to take their toll on SMFIs around the country.

> The compliance burden continues to rise. We cannot discount the impact of using limited resources to combat cybersecurity risks when so much time, energy, and money are being spent today on operational compliance issues, training, and staff time. (Source: Daryll Lund, President and CEO, Community Bankers of Wisconsin.)

2. SMFIs and SMEs Lack Sufficient Cybersecurity Resources.

As we have discussed, cyber crime is now big business. There is every reason to believe that cyber crooks will continue to find ways to defeat controls and attempt to hack small- and medium-sized businesses and high net worth individuals. To date, one of the most effective deterrents has been in educating customers, "know your customer" and placing per transaction and aggregate daily limits on ACH and wire transfers. Smaller financial institutions are generally in a better position than large institutions to know their customers, enforcing lower transaction and aggregate limits, and placing more restrictive controls involving ACH and wire transfer controls. However, smaller financial institutions cannot afford to put in place the highly sophisticated equipment that the large financial institutions use to monitor data/cybersecurity exposures. Smaller financial institutions generally do not have the resources to continually put in place the most advanced security controls. However, the solution for the smaller financial institutions is to form strategic partnerships with organizations that have expertise and infrastructure to combat the latest cyber threats. This of course requires a system for procedural controls and continuous monitoring of vendors, more effective risk management tools honed to the

unique needs of small- and medium-sized financial institutions, and normative data to help decision makers understand trends, anomalies and the like to support cost-effective information security spending.

In addition, SMFIs and SMEs typically lack information security staff. At a SMFI, a loan officer, head teller, VP of Operations, or IT staff are the usual candidates named Information Security Officer. We have yet to meet a SMFI Information Security Officer with a formal education in information protection. Bachelor, Masters, and Doctoral programs are available in Computer and Network Security, Information Security, Information Assurance, Homeland Security, and other derivatives of cybersecurity; yet, because demand simply outpaces supply, the SMFIs are left without qualified resources. Further, the Information Security Officer that is named typically wears four or five "hats" at the SMFI. Understanding emerging security threats, threat actors, vulnerabilities, and the like takes time and expertise, and cannot simply be assigned likely to existing staff.

Further, we applaud the President for inclusion of CNCI Initiative #8: Expand Cyber Education in his comprehensive strategy. While technology is vital to preventing, detecting, and responding to security attacks, equally important are the people who determine security strategy, devise and operationalize security programs, and skillfully deploy the technologies that wall-off our critical infrastructures and information. We commend the Federal Government for starting the NSA/DHS Center of Academic Excellence in Information Assurance Education and Research Programs. The NSA/DHS partnership was formed in 2004 in response to the *President's National Strategy To Secure Cyberspace of 2003.* The CAE–R program was added in 2007 to encourage universities and students to pursue research, development and innovation in Information Assurance (cybersecurity). The program originally created by this partnership has continued to grow and become even more relevant and critical to U.S. national security today. One-hundred-and-six universities across the United States, located in 37 States, the District of Columbia, and the Commonwealth of Puerto Rico, are now designated by NSA/DHS as National Centers of Academic Excellence in Information Education and/or Research. Qualified IA professionals from the National Security Agency, the Department of Homeland Security, and the Committee on National Security Systems review and assess applications. Universities designated as National Centers of Academic Excellence in Information Assurance are eligible to apply for scholarships and grants through both the Federal and Department of Defense Information Assurance Scholarship Programs. Graduates from Information Assurance programs at CAE institutions become the professional cybersecurity experts protecting national security information systems, commercial networks, and critical information infrastructure. These professionals are helping to meet the increasingly urgent needs of the U.S. Government, industry, academia, and research. Designation as a CAE/IAE or CAE–R is awarded for 5 academic years, after which the college or university must successfully reapply in order to retain the designation.

- CAE2Y—National Centers of Academic Excellence in Information Assurance 2-Year Education
- CAE/IAE—National Centers of Academic Excellence in Information Assurance Education
- CAE–R—National Centers of Academic Excellence in Information Assurance Research

The CAE program is a huge success and the credit goes to the thought leaders in the Federal Government that anticipated the cybersecurity issue and the resource shortage it would create. We advise the President to consider expanding this program with funding so that more educational, research, and outreach capacity is created to serve the needs of Government and industry (companies small and large). We advise the expansion of the scholarship for service program (SFS) at NSA, DoD, and NSF, including expanding the number of scholarships and the places scholarship students can pay back their scholarship. For example, can we make it possible for a SFS student to complete his/her service at a critical infrastructure owned and operated by the private sector? NSA and DHS alike deserve a lot of credit for operationalizing this successful program, and we suggest Administration considers leveraging this investment as a starting point for CNCI Initiative #8: Expand Cyber Education, rather than creating a new mousetrap and starting over.

More effective training and educational programs must be made available to SMFI and SME industry personnel. One such example is the program in Bank Technology Management that Kirby Davidson at the Graduate School of Banking at the University of Wisconsin has developed. This program launched in April 2011, and was capped at 50 students (which filled in 2 weeks). The program is a blend

of technology and security honed specifically to the community banking audience. The program includes 12 hours of "ethical hacking," where students download and execute common hacking tools so they understand what tools the adversary has in the arsenal.

> As the technologies used to support banking become more important, and as banking products demand more sophisticated technology solutions, it's vital that IT professionals and information security officers understand how to effectively choose, deploy and lead the use of current and emerging technologies to meet business goals and regulatory requirements. It's also critical that IT professionals understand key steps that they can initiate at their bank to proactively protect vital customer information from cyber and network attacks. All of this, and more, is included in the new Bank Technology Management School offered through the Graduate School of Banking at the University of Wisconsin-Madison. The school uses a mix of lectures, small group discussions and interactive computer simulation labs that allow students to work with learned concepts in real-world situations. (Kirby Davidson, President and CEO, Graduate School of Banking, Madison, WI.)

Small- and medium-sized financial institutions lack qualified security experts to protect their interests. SMFIs simply cannot afford or do not have access to security specialists. Many certified and qualified security officers command six-figure salaries, inconsistent with the resources available at SMFIs. Most of these certified, qualified individuals live in urban areas, again inconsistent with the demands of SMFIs. Universities, community colleges and trade schools can do even more to create programs that produce security experts who can work into the SMFI environment. As the Federal Government continues hiring of cyber experts, this will likely put even more pressure on the supply of such experts needed in SMFIs.

3. Digital Infrastructure Is Infrastructure.

When an ice storm occurs in North Dakota, icing up power lines and taking out power, the region is paralyzed until power is restored. It can sometimes take weeks and months to complete this task, depending upon the tenacity of Mother Nature. What would happen to these financial institutions, our economy, and our consumer confidence level if malicious nation-states disrupted our power instead of an ice storm? How long would it take for power to be restored on infrastructure dating back centuries?

Power, water, transportation, and the Internet (just to name a few) are all required to conduct banking commerce. While SMFIs are required to devise business continuity, incident response, and pandemic preparedness plans, no SMFI could operate if essential infrastructure we all depend up (such as the power grid) was compromised. The job is much larger than any one SMFI. The CNCI's major goals to establish a front line of defense against today's immediate threats and to defend again a full spectrum of (future) threats is so massive that only the Federal Government could take this on. However, to the degree major and minor changes are needed at SMFIs or SMEs, we urge the Administration to consider this infrastructure and fund it. There needs to be a mind-set shift away from industry paying for everything in this infrastructure (because they created it and are the users of it) to some shared cost model. If this infrastructure is truly a matter of national security then the Federal Government has a funding responsibility. Just as tanks, planes, and weapons are funded to protect our interests, we urge the Administration to consider their financial responsibilities as it relates to this vital electronic infrastructure. President Obama said it best:

> We count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control . . . But just as we failed in the past to invest in our physical infrastructure—our roads, our bridges and rails—we've failed to invest in the security of our digital infrastructure . . . This *status quo* is no longer acceptable—not when there's so much at stake. We can and we must do better. (Source: President Obama, May 29, 2009.)

Conclusion

Electronic banking is the future, and if SMFIs cannot understand and resource their technology and security requirements then they will likely be left behind. We agree with the White House's conclusion in their recent cybersecurity legislative proposal that, at least with respect to cyber terrorists, the vulnerability of the electricity grid poses one of the most severe exposures to our country's critical infrastructure. The fact that a computer programmer in another country could cause the partial or complete disruption of this Nation's grid is, to say the least, extremely

disturbing, but is beyond the scope and expertise of SMFIs to respond. However, small- and medium-sized financial institutions need representation at the table, and we encourage the President to consider including this voice as small- and medium-sized financial institutions and businesses are the majority, not the minority, of American businesses.

Thank you for the opportunity to participate in this important and timely hearing. The National Center for the Protection of the Financial Infrastructure and Dakota State University look forward to working with all stakeholders to operationalize the President's vision of a safe electronic infrastructure for all businesses to use. We applaud the President in making cybersecurity an Administration priority, and concur with the President's comments that the "cyber threat is one of the most serious economic and national security challenges we face as a Nation." To make an impact, policy must change, resource allocation must change, and a more comprehensive approach must be deployed.

We want to thank you again for this opportunity to appear before you.

PREPARED STATEMENT OF STUART K. PRATT

PRESIDENT AND CHIEF EXECUTIVE OFFICER, CONSUMER DATA INDUSTRY ASSOCIATION

JUNE 21, 2011

Chairman Johnson, Ranking Member Shelby, and Members of the Committee, my name is Stuart Pratt, and I am president and CEO of the Consumer Data Industry Association (CDIA). Thank you for this opportunity to testify on cybersecurity and data protection in the financial sector.

CDIA is an international trade association with more than 190 member companies, providing our Nation's businesses with the data tools necessary to manage risk in a wide range of consumer transactions. These products include credit and mortgage reports, identity verification tools, law enforcement investigative products, fraudulent check transaction identification systems, employment screening, tenant screening, depository account opening tools, decision sciences technologies, locator services, and collections. Our members' data and the products and services based on it ensure that consumers benefit from fair and safe transactions, broader competition and access to a market which is innovative and focused on their needs. We estimate that the industry's products are used in more than nine billion transactions per year.

You have asked us to address a number of topics in our testimony. Let me start with an overview of some of the most relevant laws and regulations which apply to our members' products and services.

Data Security

The Senate Banking Committee has a clear record across many Congresses of oversight of the financial services sector's efforts to secure sensitive personal information. Let me describe just a few of these efforts.

One of the most notable and prescient actions of the Committee was the 1999 passage of Title V of the Gramm-Leach-Bliley Act, signed into law by President Clinton. While Title V established a number of new duties relative to how data transfers occur in the financial services sector, most notable for today's hearing was the direction given to bank regulatory agencies and the Federal Trade Commission in section 501 to develop regulations regarding the security of nonpublic personal information.

The FTC's explanation of the Safeguards Rule, which implements the security requirements of the GLB Act, speaks to the breadth of the rule's application and what is required of any person who must comply:

> [It] requires financial institutions to have reasonable policies and procedures to ensure the security and confidentiality of customer information. The "financial institutions" covered by the Rule include not only lenders and other traditional financial institutions, but also companies providing many other types of financial products and services to consumers. These institutions include, for example, payday lenders, check-cashing businesses, professional tax preparers, auto dealers engaged in financing or leasing, electronic funds transfer networks, mortgage brokers, credit counselors, real estate settlement companies, and retailers that issue credit cards to consumers.
>
> The Rule is intended to be flexible to accommodate the wide range of entities covered by GLB, as well as the wide range of circumstances companies face in securing customer information. Accordingly, the Rule requires financial institutions to implement a written information security program that

> is appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its program, each financial institution must also: (1) assign one or more employees to oversee the program; (2) conduct a risk assessment; (3) put safeguards in place to control the risks identified in the assessment and regularly test and monitor them; (4) require service providers, by written contract, to protect customers' personal information; and (5) periodically update its security program.

It is hard to overstate the effects that this action has had on the security of the flows of sensitive personal information in the United States. CDIA's members operate as financial institutions under GLB and thus comply with the Safeguards Rule. The model that this Committee established more than a decade ago has withstood the test of time. It should operate as a framework for other committees as they consider establishing a similar data security duty.

Of particular importance to the CDIA is that the Senate Banking Committee had the foresight to ensure that data security was not a hard-coded statutory prescription. Risks change over time and so too must the strategies used to mitigate these risks. The Committee also recognized that those who have a duty to comply will vary in terms of size, complexity, and even the types of data retained. Because of this, the Committee built into the statute direction for regulators to take into consideration these factors when designing the rule and measuring how each person implements its requirements. This "regulatory flexibility act like" approach has been critical to ensuring strong security, by not dictating a single solution or approach to security threats, thus leaving our members' security experts the creative room to secure data assets against threats. At the same time, its flexibility is not a statutory and regulatory regime which drives small- and medium-sized businesses out of the marketplace.

The GLB Safeguards Rules are also designed to be administratively enforced, which we believe has ensured that national uniformity has not been impaired by private actions that could create a circuit-by-circuit compliance nightmare for U.S. businesses operating on a super-regional or nationwide basis. This is not to say, however, that such laws are not enforceable. For financial institutions subject to regulatory examination by bank agencies, compliance with the GLB Safeguards Rule is an annual event measured with prudence and care. For persons not subject to bank agency examinations, the Federal Trade Commission has proven itself to be an able agency in many ways. First, it has sought to encourage successful compliance through education. CDIA applauds this education-first approach which compliments the Association's own training programs on this subject. FTC enforcement actions have focused on both smaller and larger institutions, and consent orders have informed the broader community regarding approaches to compliance and FTC expectations. Overall, the GLB Safeguards Rules have operated just as expected, and have ensured that literally trillions of data transmissions and transactions are secure in the context of a healthy and competitive private-sector marketplace.

Disposal of Records

The Senate Banking Committee's accomplishments are not limited to the enactment of Title V of GLB. In 2003, as part of its extensive oversight of the Fair Credit Reporting Act, the Committee recognized that disposing of sensitive data, whether stored electronically or otherwise, should be addressed. As part of the Fair and Accurate Credit Transactions Act of 2003, Congress amended the Fair Credit Reporting Act by adding Section 628 [15 USC 1681w] entitled "Disposal of Records." This enactment required the Federal Trade Commission (as well as the Federal banking agencies, NCUA and SEC) to promulgate rules regarding the proper disposal of "consumer information, or any compilation of consumer information, derived from consumer reports." This duty expanded the concept of proper disposal of records beyond the borders of users of consumer reports who were already subject to duties under the GLB Safeguards rule. This simple, straight-forward duty, it brought tens of thousands of users of data under the new law and specific rules. In doing so, the Committee ensured that sensitive personal data about consumers wasn't simply left in a dumpster, or on the hard drive of a laptop or a hand-held device which was sold without concern for its contents.

Credentialing Customers

As a result of this Committee's actions to enact the FCRA (1970) and Title V of GLB (1999), our members have a number of duties to ensure that they know their customers, which is yet another important part of ensuring that a full and complete data security program is in place. Section 607(a) of the FCRA requires our members when operating as consumer reporting agencies to have each customer certify the

uses for which they will order consumer reports. Today, this certification process often involves on-site inspections of the customer's offices, reviewing and confirming other credentials such as business licenses, and cross-referencing a prospective customer with the SDN list and other lists administered by the U.S. Treasury's Office of Foreign Assets Control. Further, the GLB Safe Guards Rules issued by bank agencies and the FTC require that proper access controls be in place to protect against unlawful access to nonpublic personal information. Access control strategies may include details of how passwords are administered, the frequency with which they are changed, how many factors are used to authenticate a legitimate user or the use of technologies to detect possible fraudulent access.

Aligning Current Law With Cybersecurity Proposals

You have asked us to comment on how proposals, such as the Administration's cybersecurity bill, would affect financial institutions that come under the Committee's jurisdiction.

Clearly because of the leadership of the Senate Banking Committee in establishing data security requirements found in laws such as the FCRA and Title V of GLB, as well as extensive regulations and guidance issued by bank agencies which resulted from these enactments, cybersecurity risks for financial institutions and their customers are far less than would otherwise be the case. Our members already invest heavily in defending against attacks by deploying external resources, leading-edge technologies and internal data security teams with unique core competencies. Some of our largest members also participate in existing information sharing systems such as the Financial Services Information Sharing and Analysis Center. [1]

With the existing legal and regulatory framework in mind, CDIA's members recognize that risks remain, and we do believe it is appropriate for the Administration and the Congress to focus on the ever-changing mix of risks posed by cybersecurity threats. We believe, however, that it is important for new laws not to impinge on frameworks of law which already establish the necessary focus on data security. Such conflicts are not inevitable and do not have to impede the passage of new national cybersecurity protections.

As an example of how conflicts can be avoided, in place of 47 existing State laws the Administration's bill proposes to protect the American people by creating a single, national standard for how and when a notification should be sent to a consumer if there has been a breach of sensitive personal information that could pose a risk. CDIA is on record testifying as recently as this past week in support of establishing an appropriate national standard for breach notification. We look forward to contributing our experience and expertise to any effort to structure a standard that is uniform and effective for consumers. Part of ensuring that such a standard is effective is to avoid arbitrarily overwriting existing national standards that are effective today—such as data breach guidance already issued by bank agencies.

The "financial sector" is considered part of the "Nation's critical infrastructure" according to the Administration's May 12, 2011, release. As described above, the financial services industry (including CDIA's members) is heavily regulated in general and specifically with regard to securing sensitive personal information. It is not clear, however, how a "critical infrastructure" designation as determined by the Department of Homeland Security would operate in the context of new agencies such as the Consumer Financial Protection Bureau created by the Dodd Frank Act, and the existing bank agencies that have a leading mission when it comes to data security or even the Federal Trade Commission. Avoiding conflicts is necessary and will require the Senate Banking Committee to proactively engage on the broad topic of cybersecurity to ensure that current, effective laws, regulations, and guidelines for the financial services industry continue to operate coterminous with new data security or data breach notification duties that may be established for other critical infrastructure identified by DHS.

Data Security and Privacy Are not the Same Issue

The Senate Banking Committee can also play a vital role in ensuring that the important work of reducing the risks of cybersecurity attacks are not distracted by privacy issues, such as data collection and use practices. Several Congressional committees have delved into this privacy arena in an effort to address the data collection and use practices of so-called "information brokers." It is important to understand that information brokers provide the data services and products necessary for commercial entities.

---

[1] ISACs were created as a result of Presidential Decision Directive 63 (PDD-63) in 1998. The directive created a public/private-sector partnership to share information about physical and cyber threats.

Our members' products and services are particularly essential to the financial services sector. Financial institutions offering credit need to detect and prevent fraud, including identity theft, and to verify the identities of individuals seeking products and services through increasingly common remote transactions such as through the Internet, over mobile services, through the telephone and even by direct mail. CDIA members also help financial institutions enforce contracts with customers who have the ability to pay, but don't choose to do so. Lenders who must comply with bankruptcy code requirements to cease dunning a consumer who has filed for protection use our members' data tools to comply. USA Patriot Act Section 326 duties demand that financial institutions properly identify their customers and again it is our members' products and services which help them accomplish this goal and reduce the downstream effects of stolen data and other criminal efforts.

Conclusion

Let me conclude with just a few summative points:

1. As stated above, CDIA has been on record for more than a decade in support of establishing uniform, national standards for data security and data breach notification. Action on cybersecurity law could advance this cause.
2. Eliminating possible conflicts between the laudable and important goal of ensuring that the Nation is secure from cybersecurity risks and the operation of effective current data security and breach notification laws/regulations/guidance which govern the financial services sector can be accomplished with the involvement of this Committee.
3. Keeping the privacy and data security debates separate is vital to ensuring the continuance of data products and services which contribute to preventing the crimes which arise from data/cybersecurity risks and ensuring that the important work of mitigating cybersecurity risks is not encumbered by policy issues that are not relevant.

Our members again thank you for the opportunity to testify. I am happy to answer any questions.

PREPARED STATEMENT OF LEIGH WILLIAMS

BITS PRESIDENT, ON BEHALF OF THE FINANCIAL SERVICES ROUNDTABLE

JUNE 21, 2011

Thank you Chairman Johnson, Ranking Member Shelby, and Members of the Committee for the opportunity to testify before you today.

My name is Leigh Williams and I am president of BITS, the technology policy division of The Financial Services Roundtable. BITS addresses issues at the intersection of financial services, technology and public policy, on behalf of its 100 member institutions, their millions of customers, and all of the stakeholders in the U.S. financial system.

From this perspective, I will briefly describe cybersecurity and data protection in financial services, including private sector efforts, sector-specific oversight and intersector interdependencies. I understand that the Committee is considering the cybersecurity legislative proposal delivered by the Obama administration to the President of the Senate on May 12. I will explain why The Financial Services Roundtable supports that proposal, and I will comment on how the proposal can best leverage our current protections.

Financial Institutions' Voluntary Cybersecurity Efforts

In my view, within the financial services sector, the greatest amount of cybersecurity protection arises from voluntary measures taken by individual institutions for business reasons. To protect their retail customers, commercial clients, and their own franchises, industry professionals—from Chief Information Security Officers to CIOs to CEOs—are increasingly focused on safeguards, investing tens of billions of dollars in data protection. They recognize the criticality of confidentiality, reliability, and confidence to their success in the marketplace. This market-based discipline is enforced through an increasingly informed consumer base, and by a very active commercial clientele that often specifies security standards and negotiates for audit and notification rights.

At the industry level, BITS and several other coalitions facilitate a continuous process of sharing expertise, identifying and promoting best practices, and making these best practices better, to keep pace in a dynamic environment. For example,

as BITS and our members implement our 2011 business plan, we are addressing the following items associated with protecting customer data:

- Security standards in mobile financial services.
- Protection from malicious or vulnerable software.
- Security in social media.
- Cloud computing risks and controls.
- Email security and authentication.
- Prevention of retail and commercial account takeovers.
- Security training and awareness.

While all of this institution-level and industry-level effort is voluntary—not driven primarily by regulation—it is not seen by industry executives as discretionary or optional. The market, good business practices and prudence all require it.

Oversight

To strengthen public confidence and to ensure consistency across a wide variety of institutions, self-regulatory organizations and Government agencies codify and enforce a comprehensive system of requirements. Many of these represent the distillation of previously voluntary best practices into legislation introduced in this Committee, enacted into law, detailed in regulation, enforced in the field, with feedback to the Committee.

For example, Members of this Committee are very familiar with the provisions of Gramm-Leach-Bliley, the Financial Services Modernization Act of 1999 (GLB). GLB fostered the promulgation of Regulation P by the Federal Financial Institutions Examinations Council (FFIEC) and Regulation S–P by the Securities and Exchange Commission (SEC). These regulations were translated into examination guidance. That guidance is consulted by institutions as they manage security and privacy programs, comprised of risk assessments, strategic plans, control teams, authentication technologies, customer notices, and many other elements. These elements are then audited by on-site examiners, who enforce the underlying requirements and promote safety and soundness in the institutions and across the industry. The sector-wide impact is assessed by our sector-specific agency, the U.S. Department of the Treasury. Finally, bringing the process full circle, this Committee oversees the agencies.

In addition to these Federal authorities, institutions are subject to self-regulatory organizations like the Financial Industry Regulatory Authority (FINRA), State regulators like the banking and insurance commissioners, independent auditors, outside Directors, and others.

These various oversight bodies, in addition to applying GLB, also apply the Fair and Accurate Credit Transactions Act (FACTA), Electronic Funds Transfers (Regulation E), Suspicious Activity Reporting (SARs), the International Organization for Standardization criteria (ISO), the Payment Card Industry Data Security Standard (PCI), BITS' own Shared Assessments and many, many more regulations, rules, guidelines, and standards.

Inter-Sector Collaboration

Commensurate with the escalating cybersecurity challenges and increasing interconnectedness among sectors, more and more of our work entails public/private and financial/nonfinancial partnerships. Our Financial Services Sector Coordinating Council (FSSCC) of 52 institutions, utilities and associations actively partners with the seventeen agencies of the Finance and Banking Information Infrastructure Committee (FBIIC). (For additional detail on the FSSCC's perspective on cybersecurity, research and development, and international issues, I refer the Committee to the April 15, 2011, testimony of FSSCC Chair Jane Carlin before the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies of the House Homeland Security Committee.) Our Financial Services Information Sharing and Analysis Center (FS–ISAC) is in constant communication with the Department of Homeland Security (DHS), law enforcement, the intelligence community, and ISACs from the other critical infrastructure sectors, to address individual incidents and to coordinate broader efforts.

Other examples of collaboration with nonfinancial partners, drawn just from BITS' 2011 agenda, include:

- The Cyber Operational Resiliency Review (CORR) pilot, in which institutions may voluntarily request Federal reviews of their systems, in advance of any known compromise—with DHS and the Treasury.

- Multiple strategies for enhancing the security of financial Internet domains—with the Internet Corporation for Assigned Names and Numbers (ICANN) and Verisign, in partnership with the American Bankers Association (ABA) and in consultation with members of the FFIEC.
- A credential verification pilot—with DHS and the Department of Commerce—building on private sector work that began in 2009, was formalized in a FSSCC memorandum of understanding in 2010, and was featured in the April 15, 2011, announcement of the National Strategy for Trusted Identities in Cyberspace (NSTIC).

Through the processes and initiatives above and in many other efforts, financial institutions, utilities, associations, service providers, and regulators continue to demonstrate a serious, collective commitment to strengthening the security and resiliency of the overall financial infrastructure. As the Committee considers action on cybersecurity, I urge Members to be conscious of the protections and supervisory structures already in place and the collaborations currently underway, and to leverage them for maximum benefit.

Need for Legislation

Even given this headstart and substantial momentum, we believe that cybersecurity legislation is warranted. Strong legislation can catalyze systemic progress in ways that are well beyond the capacity of individual companies, coalitions or even entire industries. For example, comprehensive legislation can:

- Raise the quality and consistency of security throughout the full cyber ecosystem, including the telecommunications networks on which financial institutions depend.
- Enhance confidence among U.S. citizens and throughout the global community.
- Strengthen the security of Federal systems.
- Mobilize law enforcement and other Federal resources.
- Enable and incent voluntary action through safe harbors and outcome-based metrics, rather than relying primarily on static prescriptions.

Attached to my testimony is a list of 13 policy approaches that the FSSCC recently endorsed, along with three that it deemed problematic. I urge the Committee to consider the FSSCC's input, particularly in light of the FSSCC's leadership of the financial services industry on this issue.

Obama Administration Proposal

On May 12, 2011, on behalf of the Administration, the Office of Management and Budget transmitted to Congress a comprehensive legislative proposal to improve cybersecurity. The Financial Services Roundtable supports this legislation and looks forward to working for its passage. We support many of the provisions of this proposal on their individual merits, and we see the overall proposal as an important step toward building a more integrated approach to cybersecurity. Given that our member institutions operate nationally, are highly interdependent with other industries, and are already closely supervised by multiple regulators, we appreciate that this proposal promotes uniform national standards, throughout the cyber ecosystem, with the active engagement of sector-specific agencies and sector regulators.

Consistent with its comprehensive approach, the proposal strives to address cybersecurity both at the level of the entire ecosystem and also within specific sectors. For example:

- The Law Enforcement title refers to damage to critical infrastructure computers, but also to mail fraud and wire fraud.
- The Data Breach Notification title refers to sensitive personally identifiable information and Federal Trade Commission (FTC) enforcement, but also more specifically to financial account numbers, credit card security codes, the Fair Credit Reporting Act (FCRA), and an exclusion for entities covered under the Health Information Technology for Economic and Clinical Health Act (HITECH).
- The DHS Cybersecurity Authority title naturally stresses DHS' role, but it also mentions "other relevant agencies" and sector coordinating councils.
- Finally, the Regulatory Framework title focuses largely on DHS leadership and standardized evaluations, but it also mentions ISACs and sector-specific regulatory agencies, and provides for sector-level exemptions.

We believe that harmonizing the comprehensive approach with the need to incorporate sector-specific mechanisms will be one of the most important challenges as

the Congress considers this proposal. We urge the Committee and the full Congress to leverage existing financial services protections and circumstances, and their analogs in other sectors, while preserving the comprehensive quality of the proposal. We offer the following two approaches as illustrations:

- *Establish a uniform standard with specified exceptions:* In the Data Breach Notification title, the FTC could enforce the requirements enacted under this bill, but defer to sector-specific regulators where substantially similar sector-specific rules and guidelines already are in place (*e.g.,* the FFIEC could continue to enforce its 2005 interagency guidance, and the Department of Health and Human Services could continue to enforce HITECH).
- *Preserve sector autonomy with centralized information aggregation and coordination:* In the Regulatory Framework title, rather than requiring DHS to list critical infrastructure entities for every sector, the sector-specific agencies could make that determination, just as the Financial Stability Oversight Council is responsible for designating Systemically Important Financial Institutions.

Given the likely fluidity of the overall solution, we cannot yet make a definitive recommendation for either approach. We do believe that this question of sector/ecosystem balance warrants careful deliberation.

I will structure the remainder of my testimony as a brief commentary on a few key provisions of the proposal.

Law Enforcement

We support the proposal's clarification and strengthening of criminal penalties for damage to critical infrastructure computers, for committing computer fraud, and for the unauthorized trafficking in passwords and other means of access. We also urge similar treatment for any theft of proprietary business information. With this extension, the law enforcement provisions will improve protections for both consumers and institutions, particularly when paired with expanded law enforcement budgets and the recruitment of personnel authorized in later titles.

Data Breach Notification

We support the migration to a uniform national standard for breach notification. Given existing State and financial services breach notification requirements, this migration will require both strong preemption and reconciliation to existing regulations and definitions of covered data. We support the exemptions for data rendered unreadable, in breaches in which there is no reasonable risk of harm, and in situations in which financial fraud preventions are in place.

DHS Authority

We believe that two areas mentioned in this section—fostering the development of essential technologies, and cooperation with international partners—merit considerable investment. As DHS and the National Institute of Standards and Technology (NIST), pursue their research and development agendas, and as the Administration pursues its recently announced International Strategy for Cyberspace, we hope to see substantial resource commitments and advances in these areas.

Federal Information Security Policies

We are encouraged by the proposal of a comprehensive framework for security within Federal systems. As institutions report more and more sensitive personal and financial data to regulators (and directly and indirectly to DHS), it is critically important that this data be appropriately safeguarded. Protecting this data, modeling best practices, and using Federal procurement policies to expand the market for secure products, are all good motivations for adopting these proposed mandates.

Personnel Authorities

Because we recognize how difficult it is to recruit the most talented cybersecurity professionals, we support the expanded authorities articulated in this section. We particularly support reactivating and streamlining the program for exchanging public sector and private sector experts.

Data Center Locations

Consistent with our view of financial services as a national market, we support the presumption that data centers should be allowed to serve multiple geographies. We encourage Congress to consider extending this logic for interstate data centers to the international level, while recognizing that the owners, operators, and clients of specific facilities and cloud networks must continue to be held accountable for their security, resiliency, and recoverability of customer data, regardless of the servers' geographic location or dispersion.

Conclusion

The Financial Services Roundtable and its members are fully committed to advancing cybersecurity and resiliency, and we very much appreciate the Senate Banking Committee's attention to this issue. For our part:

- We will continue to strengthen security with our members and partners,
- We will help answer this question of ecosystem/sector balance,
- And we will work to pass and implement the Administration's cybersecurity proposal.

Thank you for your time. I would be pleased to answer any questions you may have.

Financial Services Cybersecurity Policy Recommendations

Financial Services Sector Coordinating Council – April 15, 2011

Policy Approaches the FSSCC Supports:

- Federal leadership on a national cyber-security framework, implemented with the active involvement, judgment and discretion of Treasury and the other sector specific agencies (SSAs).
- Commitment to two-way public/private information-sharing, leveraging the Information Sharing and Analysis Centers (ISACs), the US-CERT, safe harbors, clearances, and confidentiality guarantees. This must include sharing of actionable and timely information.
- Support focused efforts to address critical interdependencies such as our sector's reliance on telecommunications, information technology, energy and transportation sectors. Continue to leverage and expand on existing mechanisms (e.g., NSTAC, NIAC, PCIS).
- Involvement of Treasury and other SSAs in cyber emergencies.
- Federal cyber-security supply chain management and promotion of cyber-security as a priority in Federal procurement.
- Public education and awareness campaigns to promote safe computing practices.
- Attention to international collaboration and accountability in law enforcement, standards, and regulation/supervision.
- Increased funding of applied research and collaboration with government research agencies on authentication, access control, identity management, attribution, social engineering, data-centric solutions and other cyber-security issues.
- Increased funding for law enforcement at the international, national, state and local levels and enhanced collaboration with financial institutions, service providers and others that are critical to investigating cyber crimes and creating a better deterrent.
- Heightened attention to ICANN and other international Internet governance bodies to enhance security and privacy protection.
- Strengthening of government-issued credentials (e.g. birth certificates, driver's licenses and passports) that serve as foundation documents for private sector identity management systems.
- Enhanced supervision of service providers on whom financial institutions depend (e.g. hardware and software providers, carriers, and Internet service providers).

- Recognize the role of Federal financial regulators in issuing regulations and supervisory guidance on security, privacy protection, business continuity and vendor management for financial institutions and for many of the largest service providers.

Policy Approaches the FSSCC Opposes:

- Detailed, static cyber-security standards defined and maintained by Federal agencies in competition with existing, private standard-setting organizations.
- Establishment of vulnerability, breach and threat clearinghouses, unless security and confidentiality concerns can be definitively addressed.
- Sweeping new authority for Executive Branch to remove access to the Internet and other telecommunications networks without clarifying how, when and to what extent this would be applied to critical infrastructure.

PREPARED STATEMENT OF MARC ROTENBERG

EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

JUNE 21, 2011

Mister Chairman and Members of the Committee, thank you for the opportunity to testify today concerning cybersecurity and data protection in the financial sector. My name is Marc Rotenberg. I am executive director of the Electronic Privacy Information Center ("EPIC") and I teach privacy law at Georgetown University Law Center.

We are grateful for the work of this Committee on the critical issues of data security and privacy protection. In my testimony this morning, I will discuss the urgency of this problem, review the current legal framework, discuss the proposed cybersecurity measures, and make a few further points about forward-looking strategies for privacy protection.

I also want to note that U.S. PIRG, a leading consumer advocacy organization, has expressed support for this statement. I would encourage the members of the Committee and their staff to communicate directly with U.S. PIRG as the legislative process moves forward.

There have been several cybersecurity proposals and legislation introduced recently. We are encouraged by these efforts, and they all represent significant steps forward in the protection of consumers' financial information. The current laws do not adequately protect consumers, and the gaps need to be filled by strong legislation. Legislation should apply breach notification regulations to financial institutions, should require authentication techniques that reduce the risk to consumers, and should not preempt stronger state laws. Additionally, we favor the development of cyber security policies that are open to public review and comment, that respect the role of the private sector, and that safeguard the rights of consumers and users.

Scope of the Cybersecurity and Data Breach Problem in the Financial Sector

In recent months, there have been many high profile data breaches in the financial sector. These breaches make clear an ongoing risk to consumers and underscore the need for stronger privacy legislation.

- In May, inadequate security measures at Citigroup exposed customer names, account numbers, and contact information for more than 360,000 customers.[1] Citigroup waited almost a month before it notified its customers.[2] Experts have warned that this disclosure of customer data will make Citigroup customers especially vulnerable to phishing attacks and other acts of fraud.[3]

[1] Eric Dash, *Citi Says Many More Customers Had Data Stolen by Hackers*, N.Y. Times (June 16, 2011), http://www.nytimes.com/2011/06/16/technology/16citi.html?_r=1.
[2] Randall Smith, *Citi Defends Delay in Disclosing Hacking*, Wall St. J. (June 13, 2011), http://online.wsj.com/article/SB10001424052702304665904576382391531439656.html.
[3] Jeremy Kirk, *Citigroup Breach Exposed Data on 210,000 Customers*, PC World (June 9, 2011), http://www.pcworld.com/businesscenter/article/229868/citigroup_breach_exposed_data_on_210000_customers.html.

- On June 15, Automatic Data Processing Inc. ("ADP"), the largest payroll processor in the world, admitted that the personal data of one of its 550,000 corporate clients was breached, but did not disclose the company that was affected.

- In late May 2011, news reports revealed that a Bank of America insider had leaked the detailed personal information of many of the bank's customers.[5] As a result of the data breach, the affected customers have lost millions of dollars from their accounts.[6] This outcome is particularly troublesome considering that Bank of America is the largest bank in the U.S.[7]

- In January of 2009, weak network security caused a breach at Heartland Payment Systems, a credit card payment processing firm.[8] The company has settled with American Express, Mastercard, Visa, and Discover due to claims raised as a result of the data security breach.[9] It is estimated that millions of consumers' personal card numbers were stolen as a result of the breach.[10]

- In July of 2008, Wells Fargo, a financial services company and one of the four largest banks in the U.S., was breached by the illegal use of a bank access code.[11] The data breach resulted in the loss of personal information of approximately 5,000 consumers.[12]

- In 2007, TJX, the largest apparel off-price department store in the U.S., announced that it had been the victim of a data breach whereby the personal data of millions of customers was stolen by hackers.[14] The company eventually settled, paying almost $10 million to states,[15] $24 million to Mastercard,[16] and $41 million to Visa.[17]

---

[5] David Lazarus, *Bank of America Data Leak Destroys Trust*, L.A. Times (May 24, 2011), http://articles.latimes.com/2011/may/24/business/la-fi-lazarus-20110524
[6] *Id*.
[7] National Information Center, *Top 50 Bank Holding Companies in the U.S.*, (March 31, 2011), http://www.ffiec.gov/nicpubweb/nicweb/top50form.aspx
[8] Taylor Buley, *Metadata: World's Biggest Data Breach*, Forbes (January 20, 2009), http://www.forbes.com/2009/01/20/data-breach-metadata-tech-security-cz_tb_0120breach.html
[9] Rachel Chitra, *Update 1- Heartland Payment, Discover Settle Data Breach Claims*, Reuters (September 1, 2010), http://uk.reuters.com/article/2010/09/01/heartlandpayment-idUKSGE6800LT20100901
[10] *Id*.
[11] The Associated Press, *Wells Fargo Data Breach Revealed*, L. A. Times (August 13, 2008), http://articles.latimes.com/2008/aug/13/business/fi-wells13
[12] *Id*.
[14] Aarthi Sivaraman, *TJX Settles Data Breach Case with U.S. States*, Reuters (June 23, 2009), http://www.reuters.com/article/2009/06/23/tjx-idUSN233656120090623
[15] *Id*.
[16] Associated Press, *TJX to Pay Mastercard up to $24M in Data Breach Settlement*, Boston Herald (April 2, 2008), http://www.bostonherald.com/business/general/view.bg?articleid=1084541
[17] Keith Regan, *TJX to Shell Out $41M in Data Breach Settlement*, E-Commerce Times (November 30, 2007), http://www.technewsworld.com/story/60554.html?wlc=1308577476

These problems are not unique to the financial sector. Other companies that have recently lost control of sensitive customer information include: Epsilon, Lockheed Martin, PlayStation, and the Southern California Medical-Legal Consultants. These breaches affected millions of consumers.[18]

According to the Identity Theft Resource Center, there have been at least 195 data breaches in 2011.[19] In 2010, there were 662 breaches and over 16 million records compromised.[20] 58 of those breaches occurred at financial institutions.[21] According to the Privacy Rights Clearinghouse, 500 million sensitive records have been breached since 2005.[22] The actual number is likely much higher, as many data breaches are never reported in the media.[23]

And of course breaches are not limited to the financial services sector. In just the last few weeks, data breaches have been reported at the CIA, the International Monetary Fund, and with the Senate's own computer network.

These problems are going to get worse. As more sensitive data moves into the cloud, as we become more dependent on electronic financial records, and more companies store vast amounts of consumer data on remote servers, the risk that personal data will be improperly disclosed or accessed will necessarily increase.

Moreover, consumers and businesses that become increasingly dependent on these services are less likely to know when problems occur than if they were to lose their own laptop or experience a break-in.

There are several risks to consumers from these data breaches. The most obvious risk is identity theft, which has been the number one consumer concern for the past decade.[24] EPIC has previously said that the financial services industry bears some blame

---

[18] Hayley Tsukayama, *Sony, Epsilon Support National Data Breach Bill*, Wash. Post. (June 3, 2011), http://www.washingtonpost.com/blogs/post-tech/post/sony-epsilon-support-national-data-breach-bill/2011/06/02/AG34tvHH_blog.html; Christopher Drew, *Stolen Data is Tracked to Hacking at Lockheed*, N.Y. Times (June 3, 2011), http://www.nytimes.com/2011/06/04/technology/04security.html?_r=3; Press Release, Southern California Medical-Legal Consultants, Possible Data Breach Discovered and Contained (June 11, 2011), http://www.scmlc.com/press.htm; Liana B. Baker & Jim Finkle, *Sony Playstation Suffers Massive Data Breach*, Reuters (Apr. 26, 2011), http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426

[19] Identity Theft Resource Center, 2011 Data Breach Stats 7 (June 7, 2011), http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202011.pdf.

[20] *Id*.

[21] Linda McGlasson, *2010 Data Breach Timeline*, (December 28, 2010), http://www.bankinfosecurity.com/articles.php?art_id=2378&opg=1.

[22] Privacy Rights Clearinghouse, *500 Million Sensitive Records Breached Since 2005,* http://www.privacyrights.org/500-million-records-breached (August 26, 2010).

[23] *Id*.

[24] Federal Trade Commission, FTC Releases List of Top Consumer Complaints in 2010, http://www.ftc.gov/opa/2011/03/topcomplaints.shtm; Federal Trade Commission, FTC Releases List of Top Consumer Complaints in 2009, http://www.ftc.gov/opa/2010/02/2009fraud.shtm; Federal Trade Commission, FTC Releases List of Top Consumer Complaints in 2008, http://www.ftc.gov/opa/2009/02/2008cmpts.shtm; Federal Trade Commission, FTC Releases List of Top

for identity theft concerns because the credit granting system and electronic payment mechanisms are designed in a way that makes committing fraud easy.[25] The industry favors convenience over security because tolerating some identity theft is often more profitable for companies.[26]

We have also cautioned against the financial services industry's solution of requiring more personal information, including biometric systems, to authorize charges. These systems raise serious privacy and security risks.[27] Instead, we suggest that the best way to minimize the problem of identity theft is to reduce the industry's use of the social security number as a personal identifier.[28]

Unfortunately, identity theft is only one risk from unauthorized access to personal information. [29] Unauthorized access may be gained for other purposes that cause harm to the individual, such as stalking, corporate espionage, extortion, or to supply information that will be used for future phishing or fraud activities.

The recent breach at Citigroup is a good example of this. The information originally obtained in the breach may not have included social security numbers, credit card numbers, or other traditional tools of identity theft, but it was enough to leave consumers vulnerable to phishing attacks. Spear phishing is a more effective and targeted version of phishing as the source of the e-mails sent to the potential victims comes from a supposedly trusted or known source.[30] In instances such as this, consumers should be notified so that they can take proper precautions against future attacks and possible fallout from the data breach.

To address similar problems in the communications sector, EPIC has recommend several security measures that telecommunications firms could use to protect the privacy of customer data.[31] These measures include: authentication by consumer-set passwords instead of biographic identifiers like date of birth or social security number; audit trails that record all instances where a customer's record is accessed; encryption of stored data; notice to the affected individuals and the relevant agency when there is a security breach; and limiting data retention by either deleting call records after they are no longer needed or divorcing identification data from the transactional data.[32] Similar security measures should be applied in the financial sector.

Consumer Complaints in 2007, http://www.ftc.gov/opa/2008/02/fraud.shtm.

[25] EPIC, Identity Theft, http://epic.org/privacy/idtheft/ (last visited June 17, 2011).

[26] *Id*.

[27] *Id*.

[28] *Id*.

[29] EPIC, *Testimony for the Legislative Hearing on "Data Security: The Discussion Draft of Data Protection Legislation"*(July 29, 2005), http://epic.org/privacy/choicepoint/datasec7.28.05.html.

[30] Ross Kerber and Diane Bartz, *Analysis: Data Breach Shows New "Spear-Phishing" Risk*, Reuters (April 5, 2011), http://www.reuters.com/article/2011/04/05/us-hackers-epsilon-idUSTRE7336DZ20110405

[31] EPIC, *Petition to the Federal Communications Commission for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information* (Aug. 30, 2005) at 15, *available at* http://epic.org/privacy/iei/cpnipet.html.

[32] *Id*.

It is also important to note the related cybersecurity risks for online voting systems, as there is similar potential for abuse. I bring this to your attention because there is now an effort to promote online voting in the United States over the Internet and by fax, even thought studies have shown that these networks lack the necessary security to ensure the integrity of online voting.[33] The recent spate of attacks on US financial institutions should set off warning bells for those who favor Internet-based voting.

Current Law

There are several legal frameworks that seek to address data protection in the financial sector. But in our view, none of them provide adequate safeguards for consumers, bank customers, depositors, and others who provide personal information to obtain financial services.

The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999,[34] regulates financial institutions--businesses that are engaged in banking, insuring, stocks and bonds, financial advice, and investing. The GLBA requires these financial institutions to develop precautions to ensure the security and confidentiality of "customers' nonpublic personal information," to protect against any anticipated threats or hazards to the security or integrity of such records, and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[35]

The GLBA also codifies protections against pretexting, which is the practice of obtaining personal information through false pretenses.[36] While the GLBA imposes some data breach notification obligations on financial institutions, no specific deadline for notification is required.[37]

The GLBA is enforced by "the Federal functional regulators, the State insurance authorities, and the Federal Trade Commission with respect to financial institutions and other persons subject to their jurisdiction under applicable law."[38] There is no private right of action.

---

[33] Federal Voting Assistance Program, http://www.fvap.gov/index.html; *but see* Regenscheid, A. and Hastings, N., A Threat Analysis on UOCAVA Voting Systems, National Institute of Standards and Technology (2008) available at http://vote.nist.gov/uocava-threatanalysis-final.pdf; David Jefferson, Avi Rubin & Barbara Simons, A Comment on the May 2007 DoD Report on Voting Technologies for UOCAVA Citizens (2007) available at http://www.servesecurityreport.org/SERVE_Jr_v5.3.pdf.

[34] Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq*.

[35] 15 U.S.C. § 6801(a)-(b).

[36] 15 U.S.C. §§ 6821-6827

[37] *See* Federal Deposit Insurance Corporation, Financial Institution Letter, *Final Guidance on Response Programs,* http://ithandbook.ffiec.gov/media/resources/3391/fdi-fil-27-2005.pdf (April 27. 2005).

[38] *Id*.

Many agencies, including the Federal Trade Commission (FTC)[40] are involved with enforcing the GLBA and other financial regulations. Other enforcement entities include the Commodity Futures Trading Commission, the Department of the Treasury, the Federal Deposit Insurance Corporation, the Securities and Exchange Commission, and the National Credit Union Administration. However, enforcement has been weak. [41]

Given the GLBA's weak data breach protections and lack of strong enforcement mechanisms, there is a clear need for further legislation in this area. The Gramm–Leach–Bliley Act burdens consumers because of the opt-out standard.[42] Instead, EPIC has suggested that financial institutions implement an opt-in approach for companies' use of personal information to minimize any unwanted or unknowing disclosures of information.[43] Additionally, we support the inclusion of a private right of action to strengthen enforcement and allow individuals to seek remedies.

However, it is important to note that the opt-out standard in Gramm-Leach-Bliley was tempered by the fact that the GLBA does not contain a preemption provision, which allowed states to enact stronger laws, as discussed below.[44]

EPIC appreciates the recent efforts of the Committee to update the privacy provisions in the financial services sector. The Committee considered the Data Security Acts of 2010 and 2007, but they did not leave the Committee. The Committee marked up The Credit Rating Agency Reform Act of 2006 that was signed into law and helped prevent the misuse of nonpublic information. The Committee also held hearings on August 5, 2009 to enhance the regulation of credit rating agencies and on March 3, 2009 concerning consumer protections in financial services.

State Data Breach Laws

As of October 12, 2010, forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have all enacted data breach notification laws.[45] Most states have followed the lead of California's data breach notification law.

---

[40] The FTC does not bring many enforcement actions under the GLBA. But, under Section 5 of the FTC Act, since 2001, the FTC has brought 34 cases against businesses that failed to protect consumers' personal information. The Commission has recently recommended that legislation be passed to require companies to implement reasonable procedures to protect consumer data.

[41] *See, e.g.,* Complaint to the Federal Trade Commission by AVM, www.workingre.com/workingre/AVM-Complaint-Washington.pdf (noting that "[w]hat is not understood is the lack of enforcement by the Federal Functional Regulators identified in Sec 505 of G-L-B Act"); Allan Holmes, *The Global State of Information Security*, CIO Magazine, September 15, 2006 at 82, 91(noting that in 20065, 17% of U.S. organizations reported being out of compliance with the GLBA).

[42] EPIC, The Gramm-Leach-Bliley Act, http://epic.org/privacy/glba/ (last visited June 17, 2011).

[43] *Id*.

[44] *See* 15 U.S.C. § 6807.

[45] NSCL, State Security Breach Notification Laws (last updated Oct. 12, 2010) http://www.ncsl.org/default.aspx?tabid=13489.

Many of these laws can be traced back to the California notification law that was famously triggered in a matter that EPIC brought attention to involving the sale of data on American citizens to a criminal ring engaged in identity theft. That notification and the investigation that followed led to dramatic changes in the information broker practices in the United States. While there is clearly a lot more that needs to be done to safeguard personal data, you should not underestimate the enormous value of these breach notification statutes as well as the unintended problems that could result if federal law preempts more responsive state laws.

Current Cybersecurity Proposals

As you aware, the White House has recently introduced a series of legislative proposals to strenghten cybersecurity and to create a comprehensive framework for security standards. Several of these initiatives we favor; about others we have expressed concern. We do believe that that *Personal Data Privacy and Security Act of 2011*, which has been introduced several times before is a step in the right direction.

This bill, introduced by Senator Leahy, is designed to prevent and mitigate identity theft, to require notice of security breaches, to enhance criminal penalties, and provide other protections against security breaches, fraudulent access, and misuse of personally identifiable information.[46]

Financial institutions are exempt from major provisions of the bill, including the section providing for transparency and accuracy of data collection, as well as the data privacy and security program for personally identifiable information.[47]

The security breach notification rules in the bill would apply to financial institutions, but there is a safe harbor provision and a financial fraud prevention exemption.[48] We think this bill is an important step forward, and support the application of breach notification rules to financial institutions. At the same time, we would like to see the elimination of exemptions that weaken the bill and we have specifically recommended that federal breach notification statutes operate as a floor and not a ceiling.

Secure and Fortify Electronic Data Act (SAFE Data Act)

The SAFE Data Act, introduced by Representative Bono Mack, is a bill designed "to protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a security breach."

The Bill applies to "personal information," which includes a "financial account number, or credit or debit card number, and any required security code, access code, or

[46] Personal Privacy Data and Security Act of 2011, S.1151 (2011-2012).
[47] *Id*. at Sec. 201 (transparency and accuracy of data collection); Sec 302 (data privacy and security program for PII).
[48] *Id*. at Sec 311 and 312

password that is necessary to permit access to an individual's financial account." As such, any person who "owns or possesses data containing personal information related to that commercial activity…to establish and implement policies and procedures regarding information security practices for the treatment and protection" of that information.

However, any entity governed under title V of the Gramm-Leach-Bliley Act (GLBA) is exempt from any requirements of the SAFE Data Act for any activities governed by the GLBA.

The Act also includes requirements for data breach notification, including special requirements for third party agents and service providers.

EPIC testified last week in the House Commerce Committee about this Act.[49] EPIC supported recent changes in the bill that would require companies to act more quickly in case of breach and encourage minimization of data collection. EPIC also recommended changes in the bill to strengthen enforcement, require notification, protect identifiers linked to individuals, and ensure that state governments are able to respond on behalf of consumers as new problems emerge.

Department of Commerce Cybersecurity Green Paper

The Department of Commerce has released a Green Paper that will eventually lead to the development of "public policies and private sector norms whose voluntary adoption could improve the overall cybersecurity posture of private sector infrastructure operators, software and service providers, and users outside the critical infrastructure."

The Paper states that security standards will increase the reliability of online transactions, and references the "National Strategy for Trusted Identities in Cyberspace" (NSTIC) as a means to maintain security in sensitive transactions, including banking. The Green Paper does not otherwise impose regulate the financial industry.

White House Draft Cybersecurity Legislation

The White House Cybersecurity Legislative Proposal seeks to "improve critical infrastructure protection by bolstering public-private partnerships with improved authority for the Federal government to provide voluntary assistance to companies and increase information sharing."[50]

---

[49] *Legislative Hearing on "Discussion Draft of H.R.____, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach"* (June 15, 2011) (Testimony of Marc Rotenberg, EPIC, to House Committee on Energy and Commerce and Subcommittee on Commerce, Manufacturing, and Trade), *available at* http://epic.org/privacy/testimony/EPIC_Testimony_House_Commerce_6-11_Final.pdf.

[50] *See* White House: Legislative Language, Law Enforcement Provisions Related to Computer Security (May 12, 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf. [hereinafter "White House Legislative Proposal"].

The Proposal includes a national standard for data breach notification. Any entity that collects "sensitive personally identifiable information" (SPII) must commit to data breach notification, which pre-empts all state notification laws, whenever the SPII is "reasonably believed to have been…accessed or acquired, unless there is no reasonable risk of harm or fraud to such individual."[51] The White House Proposal defines SPII to include "a unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code," or a combination of elements that includes any of the aforementioned information.

The section on "Critical Infrastructure Cybersecurity Plans" is also relevant to the work of this Committee. The Administration deems the financial sector—along with the electricity grid and transportation networks—to be part of the critical infrastructure.[52] The Administration states that it seeks to "ensure that critical-infrastructure operators are accountable for their cybersecurity."[53]

The proposal envisions that the Department of Homeland Security (DHS) will work with the private sector to ensure that critical infrastructure operators, such as financial sector institutions, "develop their own frameworks for addressing cyber threats."[54] A third-party, commercial auditor—and the Securities and Exchange Commission, if applicable—will then review the institutions' "cybsercurity risk mitigation plans" to ensure that the plan is sufficient.[55] If the plan is inadequate, DHS can modify the plan or work with the institution to improve it.[56]

The Proposal would grant DHS the authority to develop and conduct risk assessments of Critical Information Infrastructure (CII) and foster the development…of essential information security technologies and capabilities for protecting federal systems and [CII].[59] CII is defined as "any physical or virtual information system that controls, processes, transmits, receives, or stores electronic information in any form…that is vital to the functioning of critical infrastructure, so vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on national security, *national economic security*, or national public health or safety, or owned or operated by or on behalf of a state, local, tribal, or territorial government entity."[60] This would seem to include the financial services industry in its broad sweep.

---

[51] Letter from Jacob J. Lew, Director, Executive Office of the President Office of Management and Budget, to the Honorable John Boehner, Speaker of the House of Representatives and Joseph R. Biden, President of the Senate (May 12, 2011), *available at* http://www.whitehouse.gov%2Fsites%2Fdefault%2Ffiles%2Fomb%2Flegislative%2Fletters%2FCybersecurity-letters-to-congress-house-signed.pdf.

[52] Press Release, The White House, Fact Sheet: Cybersecurity Legislative Proposal (May 12, 2011), *available at* http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] *Id.*

[59] White House Legislative Proposal, *supra* note 39 at 22.

[60] *Id*. at 20. Emphasis added.

EPIC welcomes the White House's efforts to strengthen our nation's cybersecurity and privacy protections for financial information. While the White House states that "[p]rotecting civil liberties and privacy rights remain fundamental objectives in the implementation of the [Cybersecurity Legislation],"[61] we would warn the Committee about the provisions giving control over "critical information infrastructure" (CII) to the DHS. The definition of CII is quite broad and it is important to ensure that any cybersecurity proposal does not lead to increased government monitoring of private information.

Analysis

The legislative proposals in the House and Senate exempt financial institutions covered by the GLBA from much of the significant provisions of the proposals. However, they do contain breach notification rules that would apply to banks, which would help fill the gap left by the GLBA, provided that these rules are coupled with strong meaningful enforcement from federal agencies.

In contrast, the White House Cybersecurity Proposal does not specifically exempt financial institutions or GLBA covered entities from its proposed regulations. Therefore, banks could be covered under the Proposal.

In general we favor the development of cyber security policies that are open to public review and comment, that respect the role of the of the private sector, and that safeguard the rights of consumers and users. I make this point because there is the very real risk that in the realm of cyber security much of the authority for legal compliance and technical standard-setting could be too easily turned over the National Security Agency. Already the NSA has suggested that the government may need to monitor private networks and assist in the development of key technical standards.

This would be a grave mistake. In fact, if the NSA had it's way twenty years in the battle over cryptography standards for the Internet, it is quite likely that the vulnerability of US networks to attack would be much greater than it is today. This should be of particular concern to those watching closely the recent cyber security developments in the financial services sector.

Preemption

The Senate and House data breach bills preempt state laws that have similar security obligations as well as state laws that provide for data breach notification. If enacted, the federal laws would preempt more effective state information security legislation and foreclose future legislative innovation at the state level.

My own view is that it would be a mistake to adopt preemption provisions of this

---

[61] The White House, *The Comprehensive National Cybersecurity Initiative*, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (last visited June 20, 2011).

type. Businesses understandably will prefer a single national standard. That is the argument for preemption. However privacy laws have typically created a federal baseline and allowed the states to adopt more stringent safeguards if they wish. This approach to consumer protection is based upon our federalism form of government that allows the states to experiment with new legislative approaches to emerging issues. It is important that states be permitted to legislate in this area. As discussed already, most states have comprehensive data breach legislation. Often, this legislation establishes a private right of action, statutory damage scheme, and notification requirements. [63]

Because states enjoy a unique perspective that allows them to craft innovative programs to protect consumers, they should be permitted to continue to operate as "laboratories of democracy" in the privacy and data security arena. State legislatures are closer to their constituents and the entities they regulate; they are the first to see trends and problems, and are well-suited to address new challenges and opportunities that arise from evolving technologies and business practices. This is why privacy bills have typically created a federal baseline and allowed the states to adopt more stringent safeguards if they wish.

There is an additional reason that we believe weighs against preemption in the information security field: these problems are rapidly changing and the states need the ability to respond as new challenges emerge. California and Massachusetts have recently considered updating their data breach legislation in response to new threats.[64] It is very likely that the states will continue to face new challenges in this field. Placing all of the authority to respond here in Washington in one agency would be, as some in the security field are likely to say, a "critical failure point." The temptation to establish a national standard for breach notification should be resisted, particularly given the rapidly changing nature of the problem.

Conclusion

Financial privacy protections need to be strengthened in the U.S. The rise in significant data breaches and the problem of I.D. theft indicate clearly that more must be done in this area to protect financial data.

We support legislation that strengthens safeguards for consumer information and promotes data minimization practices. Specifically, we urge the adoption of techniques that minimize the collection of personally identifiable information. These techniques reduce the risk of cyber attack and minimize the risk to consumers when attacks occur.

We broadly favor Administration efforts to promote cybersecurity. But we caution against Government overreaching that leads to increased monitoring of private

[63] *See e.g.* Cal. Civ. Code 1798.82 (2011).
[64] Jason Gavejian, *California and Massachusetts Legislatures Push Data Breach and Security Bills,* Workplace Privacy, Data Management, and Security Report (May 3, 2011), http://www.workplaceprivacyreport.com/2011/05/articles/workplace-privacy/california-and-massachusetts-legislatures-push-data-breach-and-security-bills/

communications or technical standard-setting that makes communications and databases more vulnerable to attack.

Thank you for the opportunity to testify today. I will be pleased to answer your questions.

PREPARED STATEMENT OF PABLO MARTINEZ

DEPUTY SPECIAL AGENT IN CHARGE, CRIMINAL INVESTIGATIVE DIVISION, SECRET SERVICE

JUNE 21, 2011

Good morning Chairman Johnson, Ranking Member Shelby, and distinguished Members of the Committee. Thank you for the opportunity to testify on the role of the U.S. Secret Service (Secret Service) in investigating and dismantling criminal organizations involved in cyber crime.

On February 1, 2010, the Department of Homeland Security (DHS) delivered the Quadrennial Homeland Security Review (QHSR), which established a unified, strategic framework for homeland security missions and goals. The QHSR underscores the need for a safe and secure cyberspace:

> Our economic vitality and national security depend today on a vast array of interdependent and critical networks, systems, services and resources. We know this interconnected world as cyberspace, and without it, we cannot communicate, travel, power our homes, run the economy, or obtain Government services.
>
> Yet as we migrate more of our economic and societal transactions to cyberspace, these benefits come with increasing risk. We face a variety of adversaries who are working day and night to use our dependence on cyberspace against us. Sophisticated cyber criminals pose great cost and risk both to our economy and national security. They exploit vulnerabilities in cyberspace to steal money and information, and to destroy, disrupt, or threaten the delivery of critical services. For this reason, safeguarding and securing cyberspace has become one of the Department of Homeland Security's most important missions. (p. 29) [1]

In order to maintain a safe and secure cyberspace, we have to disrupt the criminal organizations and other malicious actors engaged in high consequence or wide-scale cyber crime.

As the original guardian of the Nation's financial payment systems, the Secret Service has a long history of protecting American consumers, industries and financial institutions. Over the last two decades, the Secret Service's statutory authorities have been reinforced to include access device fraud (18 USC §1029), which includes credit and debit card fraud. The Secret Service also has concurrent jurisdiction with other law enforcement agencies for identity theft (18 USC §1028), computer fraud (18 USC §1030), and bank fraud (18 USC §1344).

Due to our extensive experience investigating financial crimes, the Secret Service participated in the President's Comprehensive National Cyber Security Initiative to raise our overall capabilities in combating cyber crime and all forms of illegal computer activity. The Secret Service developed a multifaceted approach to combating cyber crime by: expanding our Electronic Crimes Special Agent Program; expanding our network of Electronic Crimes Task Forces; creating a Cyber Intelligence Section; expanding our presence overseas; forming partnerships with academic institutions focusing on cybersecurity; and working with DHS to establish the National Computer Forensic Institute to train our State and local law enforcement partners in the area of cyber crime. These initiatives led to the opening of 957 criminal cases and the arrest of 1,217 suspects in fiscal year 2010 for cyber crime related violations with a fraud loss of $507.7 million. The arrest of these individuals prevented an additional loss estimated at $7 billion dollars and involved the examination of 867 terabytes of data, which is roughly the equivalent of 867,000 copies of the Encyclopedia Britannica. As a result of these efforts, the Secret Service is recognized worldwide for our investigative and innovative approaches to detecting, investigating, and preventing cyber crimes.

Trends in Cyber Crimes

Advances in computer technology and greater access to personal information via the Internet have created a virtual marketplace for transnational cyber criminals to share stolen information and criminal methodologies. As a result, the Secret Service has observed a marked increase in the quality, quantity, and complexity of cyber crimes targeting private industry and critical infrastructure. These crimes include network intrusions, hacking attacks, malicious software, and account takeovers leading to significant data breaches affecting every sector of the world economy.

---

[1] Department of Homeland Security. (2010). Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland.

The increasing level of collaboration among cyber criminals raises both the complexity of investigating these cases and the level of potential harm to companies and individuals. For example, illicit Internet carding portals allow criminals to traffic stolen information in bulk quantities globally. These portals, or "carding Web sites," operate like online bazaars where criminals converge to trade personal financial data and cyber tools of the trade. The Web sites vary in size, from a few dozen members to some of the more popular sites boasting membership of approximately 80,000 users. Within these portals, there are separate forums moderated by notorious members of the carding community. Members meet online and discuss specific topics of interest. Criminal purveyors buy, sell, and trade malicious software, spamming services, credit, debit and ATM card data, personal identification data, bank account information, brokerage account information, hacking services, counterfeit identity documents, and other forms of contraband.

Over the years, the Secret Service has infiltrated many of the "carding Web sites." One such infiltration allowed the Secret Service to initiate and conduct a 3-year investigation that led to the indictment of 11 perpetrators involved in hacking nine major U.S. retailers and the theft and sale of more than 40 million credit and debit card numbers. The investigation revealed that defendants from the United States, Estonia, China, and Belarus successfully obtained credit and debit card numbers by hacking into the wireless computer networks of major retailers—including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, and Dave & Buster's. Once inside the networks, they installed "sniffer" programs that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks. After the data was collected, the conspirators concealed the information in encrypted computer servers that they controlled in the United States and Eastern Europe. The credit and debit card numbers were then sold through online transactions to other criminals in the United States and Eastern Europe. The stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The defendants then used these cards to withdraw tens of thousands of dollars at a time from ATMs. The defendants were able to conceal and launder their fraudulent proceeds by using anonymous Internet-based electronic currencies within the United States and abroad, and by channeling funds through bank accounts in Eastern Europe.

In both of these cases, the effects of the criminal acts extended well beyond the companies compromised, affecting millions of individual card holders in one of the incidents. Although swift investigation, arrest, and prosecution prevented many consumers from direct financial harm, all potential victims were at risk for misuse of their credit cards, overall identity theft, or both. Further, business costs associated with the need for enhanced security measures, reputational damage and direct financial losses are ultimately passed on to consumers.

Collaboration With Other Federal Agencies and International Law Enforcement

While cyber criminals operate in a world without borders, the law enforcement community does not. The increasingly multinational, multijurisdictional nature of cyber crime cases has increased the time and resources needed for successful investigation and adjudication. The partnerships developed through our Electronic Crimes Task Forces, the support provided by our Cyber Intelligence Section, the liaison established by our overseas offices, and the training provided to our special agents via Electronic Crimes Special Agent Program were all instrumental to the Secret Service's successful investigation into the network intrusion of Heartland Payment Systems. An August 2009 indictment alleged that a transnational organized criminal group used various network intrusion techniques to breach security, navigate the credit card processing environment, and plant a "sniffer," a data collection device, to capture payment transaction data.

The Secret Service investigation—the largest and most complex data breach investigation ever prosecuted in the United States—revealed that data from more than 130 million credit card accounts were at risk of being compromised and exfiltrated to a command and control server operated by an international group directly related to other ongoing Secret Service investigations. During the course of the investigation, the Secret Service uncovered that this international group committed other intrusions into multiple corporate networks to steal credit and debit card data. The Secret Service relied on various investigative methods, including subpoenas, search warrants, and Mutual Legal Assistance Treaty requests through our foreign law enforcement partners to identify three main suspects. As a result of the investigation, the three suspects in the case were indicted for various computer-related crimes. The lead defendant in the indictment pled guilty and was sentenced

to 20 years in Federal prison. This investigation is ongoing with over 100 additional victim companies identified. The Secret Service is working with our law enforcement partners both domestically and overseas to apprehend the two defendants who are still at large.

Recognizing these complexities, several Federal agencies are collaborating to investigate cases and identify proactive strategies. Greater collaboration within the Federal, State, and local law enforcement community enhances information sharing, promotes efficiency in investigations, and facilitates efforts to de-conflict in cases of concurrent jurisdiction. For example, the Secret Service has collaborated extensively with the Department of Justice's Computer Crimes and Intellectual Property Section (CCIPS), which "prevents, investigates, and prosecutes computer crimes by working with other Government agencies, the private sector, academic institutions, and foreign counterparts."[2] The Secret Service's Electronic Crimes Task Forces are a natural complement to CCIPS, resulting in an excellent partnership over the years. In the last decade, nearly every major cyber investigation conducted by the Secret Service has benefited from CCIPS contributions. Successful investigations such as the prosecution of the Shadowcrew criminal organization, E-Gold prosecution, TJX and Heartland investigations, as well as the recent apprehension of Vladislav Horohorin, were possible as a result of this valued partnership. The Secret Service looks forward to continuing our excellent work together.

The Secret Service also maintains an excellent relationship with the Federal Bureau of Investigation (FBI). The Secret Service has a permanent presence at the National Cyber Investigative Joint Task Force where the FBI leads Federal law enforcement efforts surrounding cyber matters of national security. In the last several years, the Secret Service has partnered with the FBI on various high-profile cyber investigations.

The case of Vladislav Horohorin is another example of successful cooperation between the Secret Service and its law enforcement partners around the world. Mr. Horohorin, one of the world's most notorious traffickers of stolen financial information, was arrested in Nice, France, on August 25, 2010, pursuant to a U.S. arrest warrant issued by the Secret Service. Mr. Horohorin created the first fully automated online store which was responsible for selling stolen credit card data. Working with our international law enforcement partners, the Secret Service identified and apprehended Mr. Horohorin as he was boarding a flight from France back to Russia. Both the CCIPS and the Office of International Affairs of the Department of Justice played critical roles in this apprehension. Furthermore, as a result of information sharing, the FBI was able to bring additional charges against Mr. Horohorin for his involvement in a Royal Bank of Scotland network intrusion. We are presently awaiting Mr. Horohorin's extradition to the United States to face charges levied upon him in different districts by both the Secret Service and the FBI. This type of cooperation is crucial if law enforcement is to be successful in disrupting and dismantling criminal organizations involved in cyber crime.

One of the main obstacles that agents investigating transnational crimes encounter is the jurisdictional limitations. The Secret Service believes that to fundamentally address this issue, appropriate levels of liaison and partnerships must be established with our international law enforcement counterparts. Currently, the Secret Service operates 23 offices abroad, each having regional responsibilities to provide global coverage. The personal relationships that have been established in those countries are often the crucial element to the successful investigation and prosecution of suspects abroad.

Within DHS, the Secret Service has strengthened our relationship with the National Protection and Programs Directorate's (NPPD) United States Computer Emergency Readiness Team (US–CERT), which provides response support and defense against cyber intrusions or incidents for the Federal Civil Executive Branch (.gov) domain, as well as information sharing and collaboration with State and local government, industry and international partners. As the Secret Service identifies malware, suspicious IPs and other information through its criminal investigations, it shares information with US–CERT. The Secret Service looks forward to building on its full-time presence at US–CERT, and broadening this and other partnerships within the Department.

As a part of these efforts and to ensure that information is shared in a timely and effective manner, the Secret Service has personnel detailed to the following DHS and non-DHS entities:

- NPPD's Office of the Under Secretary;

---

[2] U.S. Department of Justice. (n.d.). Computer Crime and Intellectual Property Section: About CCIPS. Retrieved from *http://www.justice.gov/criminal/cybercrime/ccips.html*.

- NPPD's National Cyber Security Division (US–CERT);
- NPPD's Office of Infrastructure Protection;
- DHS's Science and Technology Directorate (S&T);
- Department of Justice National Cyber Investigative Joint Task Force (NCIJTF);
- Each FBI Joint Terrorism Task Force (JTTF), including the National JTTF;
- Department of the Treasury—Terrorist Finance and Financial Crimes Section
- Department of the Treasury—Financial Crimes Enforcement Network (FinCEN);
- Central Intelligence Agency;
- Department of Justice, International Organized Crime and Intelligence Operations Center;
- Drug Enforcement Administration's Special Operations Division
- EUROPOL; and
- INTERPOL

The Secret Service is committed to ensuring that all its information sharing activities comply with applicable laws, regulations, and policies, including those that pertain to privacy and civil liberties.

Secret Service Framework

To protect our financial infrastructure, industry, and the American public, the Secret Service has adopted a multifaceted approach to aggressively combat cyber and computer-related crimes. The Secret Service has dismantled some of the largest known transnational cyber-criminal organizations by:

- Providing computer-based training to enhance the investigative skills of special agents through our *Electronic Crimes Special Agent Program,* and to our State and local law enforcement partners through the *National Computer Forensics Institute*;
- Collaborating with our partners in law enforcement, the private sector and academia through our 31 *Electronic Crimes Task Forces;*
- Identifying and locating international cyber criminals involved in network intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes through the analysis provided by our *Cyber Intelligence Section*;
- Maximizing partnerships with international law enforcement counterparts through our *international field offices;* and
- Maximizing technical support, research and development, and public outreach through the *Software Engineering Institute/CERT Liaison Program* at Carnegie Mellon University.

Electronic Crimes Special Agent Program

A central component of the Secret Service's cyber-crime investigations is its Electronic Crimes Special Agent Program (ECSAP), which is comprised of nearly 1,400 Secret Service special agents who have received at least one of three levels of computer crimes-related training. These agents are deployed in more than 98 Secret Service offices throughout the world and have received extensive training in forensic identification, preservation, and retrieval of electronically stored evidence. ECSAP-trained agents are computer investigative specialists, qualified to conduct examinations on all types of electronic evidence. These special agents are equipped to investigate the continually evolving arena of electronic crimes and have proven invaluable in the successful prosecution of criminal groups involved in computer fraud, bank fraud, identity theft, access device fraud, and various other electronic crimes targeting our financial institutions and private sector.

The ECSAP program is divided into three levels of training:

Level I—Basic Investigation of Computers and Electronic Crimes (BICEP). The BICEP training program focuses on the investigation of electronic crimes and provides a brief overview of several aspects involved with electronic crimes investigations. This program provides Secret Service agents and our State and local law enforcement partners with a basic understanding of computers and electronic crime investigations and is now part of our core curriculum for newly hired special agents.

Level II—Network Intrusion Responder (ECSAP–NI). ECSAP–NI training provides special agents with specialized training and equipment that allows them to respond to and investigate network intrusions. These may include intrusions into financial sector computer systems, corporate storage servers or various other targeted platforms. The Level II trained agent will be able to identify critical artifacts that will

allow effective investigation of identity theft, malicious hacking, unauthorized access, and various other related electronic crimes.

Level III—Computer Forensics (ECSAP–CF). ECSAP–CF training provides special agents with specialized training and equipment that allows them to investigate and forensically obtain legally admissible digital evidence to be utilized in the prosecution of various electronic crimes cases, as well as criminally focused protective intelligence cases.

Electronic Crimes Task Forces

In 1995, the Secret Service established the New York Electronic Crimes Task Force (ECTF) to combine the resources of academia, the private sector, and local, State, and Federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructures. Congress further directed the Secret Service in Public Law 107-56 to establish a nationwide network of ECTFs to "prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."

The Secret Service currently operates 31 ECTFs, including two based overseas in Rome, Italy, and London, England. Membership in our ECTFs includes: 4,093 private sector partners; 2,495 international, Federal, State, and local law enforcement partners; and 366 academic partners. By joining our ECTFs, all of our partners benefit from the resources, information, expertise and advanced research provided by our international network of members while focusing on issues with significant regional impact.

Cyber Intelligence Section

Another example of our partnership approach with private industry is our Cyber Intelligence Section (CIS) which collects, analyzes, and disseminates data in support of Secret Service investigations worldwide and generates new investigative leads based upon its findings. CIS leverages technology and information obtained through private sector partnerships to monitor developing technologies and trends in the financial payments industry for information that may be used to enhance the Secret Service's capabilities to prevent and mitigate attacks against the financial and critical infrastructures.

CIS has an operational unit that investigates international cyber criminals involved in cyber intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes. The information and coordination provided by CIS is a crucial element to successfully investigating, prosecuting, and dismantling international criminal organizations.

National Computer Forensics Institute

The National Computer Forensics Institute (NCFI) initiative is the result of a partnership between the Secret Service, NPPD of DHS, the State of Alabama, and the Alabama District Attorney's Association. The goal of this facility is to provide a national standard of training for a variety of electronic crimes investigations. The program offers State and local law enforcement officers, prosecutors, and judges the training necessary to conduct computer forensics examinations. Investigators are trained to respond to network intrusion incidents and conduct electronic crimes investigations.

Since the establishment of NCFI on May 19, 2008, the Secret Service has provided critical training to 932 State and local law enforcement officials representing over 300 agencies from all 50 States and two U.S. territories.

Computer Emergency Response Team/Software Engineering Institute (CERT–SEI)

In August 2000, the Secret Service and Carnegie Mellon University Software Engineering Institute (SEI) established the Secret Service CERT Liaison Program to provide technical support, opportunities for research and development and public outreach and education to more than 150 scientists and researchers in the fields of computer and network security, malware analysis, forensic development, training and education. Supplementing this effort is research into emerging technologies being used by cyber criminals and development of technologies and techniques to combat them.

The primary goals of the program are: to broaden the Secret Service's knowledge of software engineering and networked systems security; to expand and strengthen partnerships and relationships with the technical and academic communities; to provide an opportunity to work closely with CERT–SEI and Carnegie Mellon University; and to present the results of this partnership at the quarterly meetings of our ECTFs.

In August 2004, the Secret Service partnered with CERT–SEI to publish the first ever "Insider Threat Study" examining the illicit cyber activity in the banking and finance sector. Due to the overwhelming response to this initial study, the Secret Service and CERT–SEI, in partnership with DHS S&T, are working to update the study. An updated study, expected to be released in late 2011, will analyze actual incidents of insider crimes from inception to prosecution. The research team will share its findings with Federal, State, and local law enforcement, private industry, academia and other Government agencies.

Conclusion

As more information is stored in cyberspace, target-rich environments are created for sophisticated cyber criminals. With proper network security, businesses can provide a first line of defense by safeguarding the information they collect. Such efforts can significantly limit the opportunities for these criminal organizations. Furthermore, the prompt reporting of major data breaches involving sensitive personally identifiable information to the proper authorities will help ensure a thorough investigation is conducted.

The Secret Service is committed to safeguarding the Nation's financial payment systems by investigating and dismantling criminal organizations involved in cyber crime. Responding to the growth in these types of crimes and the level of sophistication these criminals employ requires significant resources and greater collaboration among law enforcement and its public and private sector partners. Accordingly, the Secret Service dedicates significant resources to improving investigative techniques, providing training for law enforcement partners and raising public awareness. The Secret Service will continue to be innovative in its approach to cyber crime and cybersecurity and is pleased that the Subcommittee recognizes the magnitude of these issues and the evolving nature of these crimes.

Chairman Johnson, Ranking Member Shelby, and distinguished Members of the Committee, this concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service. I will be pleased to answer any questions at this time.

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

STATEMENT SUBMITTED BY THE SECURITIES INDUSTRY AND FINANCIAL MARKETS ASSOCIATION

I. Introduction

SIFMA supports the goals of President Obama and Congress to limit cybersecurity threats to the American people, businesses, and Government through a more integrated approach to fighting these threats. The increase in cyber intrusions and cyber crimes in the past decade is cause for great concern, particularly those in the financial services sector. SIFMA member firms are on the front lines of defense against cyber threats to the financial markets and we take this role very seriously. On May 12, 2011, President Obama released an extensive proposal (Proposal) which is intended to bolster the American cybersecurity infrastructure and protect Americans from cyber threats. Although SIFMA supports the ultimate goals of the Proposal, we are concerned that the Proposal does not adequately take into consideration the extensive existing regulatory framework under which the financial services industry functions.

SIFMA brings together the shared interests of more than 600 securities firms, banks, and asset managers throughout the world. By building trust and confidence in the financial industry SIFMA intends to encourage capital availability, job creation, and economic growth. Encouraging effective data protection goes to the heart of SIFMA's mission of building trust and confidence in the financial services industry. Without effective protection of the personal data of their customers, financial institutions would lack the public trust that is so critical for their operation.

SIFMA's members include some of the largest financial institutions in the world. As part of the financial services industry, SIFMA members are currently subject to stringent laws and regulation on the protection of personal data, including the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA) and the Right to Financial Privacy Act. These laws and regulations are reinforced by regular, proactive review and audit by highly specialized regulators. Consequently, SIFMA members are accustomed to and fully supportive of protecting their customers' data, and, as partners and service providers, the data of customers of financial institutions worldwide.

II. Importance of Recognizing Uniqueness of the Financial Services Sector

The United States has for decades embraced a sector-specific approach to data security and privacy regulation. As a result, health and financial information are subject to extensive regulation that was crafted for the unique circumstances presented by those industries. Applying general data security and privacy concepts to those industries is not only unnecessary, it could be inconsistent with existing regulations and produce unintended negative consequences.

SIFMA urges Congress to consider the unique position of the U.S. financial services sector in connection with the ongoing examination of national privacy framework. As discussed below, financial services firms appreciate more than almost any sector of the economy the importance of maintaining the confidentiality of customer information. The financial services industry is keenly aware of the potential for tangible harm that could flow from a privacy or security lapse, and has long played a leadership role in developing policies, procedures, and technology to protect customer data.

The financial services industry has had an effective and longstanding engagement with the U.S. Treasury Department on cybersecurity since Presidential Decision Directive/NSC–63 was issued in May 1998. In response, the industry proactively formed the Financial Services Information Sharing and Analysis Center (FS–ISAC). The industry has committed significant time and effort to integration with the Department of Homeland Security (DHS) through US–CERT and the National Cybersecurity and Communications Integration Center (NCCIC). In addition, the FS–ISAC is already in the process of embedding appropriately cleared staff in the NCCIC.

Since 1970, the FCRA has promoted the accuracy, fairness, and privacy of personal data assembled by "consumer reporting agencies" (CRAs), including data provided by a majority of SIFMA member firms. The FCRA establishes a framework of fair information practices that include rights of data quality, data security, identity theft prevention, use limitations, requirements for data destruction, notice, user consent, and accountability.

The GLBA provides data privacy rules applicable to "financial institutions," a term defined broadly to cover entities significantly engaged in financial activities such as banking, insurance, securities activities, and investment activities. The

GLBA imposes data privacy obligations such as the obligation to securely store personal financial information, and provide data subjects with notice of the institution's privacy practices and the right to opt-out of some sharing of personal financial information. The GLBA and the regulations issued under the GLBA help to protect valuable customer information and to prevent data breaches. Through exceptionally broad definitions, GLBA protections apply to virtually all personal information about individual consumers or customers held by more than 40,000 financial institutions in the United States—including less traditional "financial institutions" such as check-cashers, information aggregators, and financial software providers. Moreover, the GLBA and its implementing regulations require financial institutions not only to limit the disclosure of customer information, but also to protect that information from unauthorized accesses or uses. The GLBA regulations also provide guidelines to financial institutions on appropriate actions in response to a breach of security of sensitive data, including on investigation, containment, and remediation of the incident and notification of consumers and/or law enforcement authorities when warranted.

Many SIFMA member firms also follow the Federal Financial Institutions Examination Council (FFIEC) guidance and monitoring procedures. The FFIEC is an interagency body empowered to prescribe uniform principles, standards, and report forms for the Federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. The FFIEC also makes recommendations to promote uniformity in the supervision of financial institutions. In the area of cybersecurity and data breach protection, the FFIEC has published the following standards: FFIEC Interagency Guidelines Establishing Standards for Safeguarding Customer Information; FFIEC Interagency Guidelines Establishing Information Security Standards; FFIEC Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice; FFIEC Information Technology Examination Handbook (includes guidance and audit provisions of many of the requirements identified in the guidance documents referenced above).

Finally, many SIFMA member firms who process Government loan data must comply with the Federal Information Security Management Act of 2002 (FISMA) and the Federal Information System Controls Audit Manual 2009 (FISCAM). FISMA emphasizes the need to develop, document, and implement an enterprise-wide program to provide information security for the information and information systems that support the operations and assets of the Federal Government, including those provided or managed by another agency, contractor, or other source. FISMA directs the promulgation of Federal standards for: (i) the security categorization of Federal information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; and (ii) minimum security requirements for information and information systems in each such category.

In accordance with FISMA, the National Institute of Standards and Technology (NIST) develops the guidance and procedures which directly pertain to security control implementation, continuous monitoring, independent assessment, and risk analysis. The NIST Federal Information Processing Standard (FIPS) Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," specifies minimum security requirements for Federal information in 17 security-related areas. These minimum security requirements are defined through the use of the security controls provided by NIST Special Publication 800-53 rev3, "Recommended Security Controls for Federal Information Systems."

FISCAM is designed to be used primarily on financial and performance audits and attestation engagements performed in accordance with generally accepted Government auditing standards (GAGAS), as presented in Government Auditing Standards (also known as the "Yellow Book"). FISCAM is also consistent with the GAO/PCIE Financial Audit Manual (FAM). Additionally, FISCAM control activities are consistent with NIST Special Publication 800-53 rev3 controls.

III. Support for the Proposal

A. Improved Coordination Across Agencies and Sectors

SIFMA believes the Proposal takes many important steps to ensuring a safer cyber community and SIFMA fully supports those efforts. The Federal Government should be leading the proactive defense against cybersecurity threats and take coordinated action to protect critical infrastructure from such attacks. SIFMA members rely heavily on other sectors such as telecommunications, information technology, energy, and transportation which are frequently at risk for cyber attacks. SIFMA supports enhanced supervision over service providers on which financial in-

stitutions depend (*e.g.,* hardware and software providers, Internet service providers, *etc.*). Such coordination may be achieved by building on the existing mechanisms that seek to address these issues (*e.g.,* Partnership for Critical Infrastructure Security).

Moreover, SIFMA believes that cyber threats can be best fought through a coordinated defense network across agencies and business sectors. Such an infrastructure would improve communication and enforcement mechanisms. Coordination should occur at the agency level where agencies can report cyber threats through predetermined channels whereby threats can be reviewed and analyzed consistently, regardless of source. Individual firms should not be required to report cyber attacks and threats to multiple agencies under multiple reporting regimes. Such a structure is inefficient and may delay defensive measures.

SIFMA also supports the Administration's commitment to two-way public/private information-sharing, leveraging the Information Sharing and Analysis Centers (ISACs), the US–CERT, safe harbors, clearances, and confidentiality guarantees. As an example, the Financial Services-Information Sharing and Analysis Center (FS–ISAC) constantly gathers reliable and timely information from financial services providers, commercial security firms, Federal, State, and local government agencies, law enforcement and other trusted resources. FS–ISAC is uniquely positioned to quickly disseminate physical and cyber threat alerts and other critical information to participating organizations, including analysis and recommended solutions from leading security industry experts. SIFMA also believes there is opportunity to accelerate information flow on a cyber event without compromising sensitive information. This can be done through segmentation, protocols, and decision trees.

SIFMA also supports Federal cybersecurity supply chain management and promotion of cybersecurity as a priority in Federal procurement. Other efforts to defend against cybersecurity threats will be lessened without financial support for the infrastructure necessary to implement a defense strategy.

B. Law Enforcement

SIFMA supports the strengthening and clarification of criminal penalties for certain cyber crimes. Such expansion will provide additional protection for consumers and financial institutions from financial crimes. These improvements are further bolstered by the increase in budgets and personnel for these purposes at law enforcement agencies.

C. Technology and International Cooperation

SIFMA believes that the development of essential technologies and improving Federal systems are important efforts which should be supported. As DHS and NIST pursue their research and development agendas, and as the Administration pursues its recently announced International Strategy for Cyberspace, we hope to see substantial resource commitments and advances in these areas. SIFMA also supports the improvement of the resilience and security of Federal systems to further prevent cyber crime.

D. Cooperation With International Partners

Because cybersecurity is a global problem and cyber crimes frequently occur across borders, cooperation with international partners is critical to preventing, investigating, and prosecuting cyber crime. Without strong cooperation with international law enforcement agencies, U.S. efforts to improve cybersecurity will be severely limited.

E. Safe Harbor for Voluntary Disclosure

SIFMA members believe that the safe harbor provisions for cybersecurity reporting under Sec. 245, "Voluntary Disclosure of Cybersecurity Information," will be helpful for SIFMA members and provide much-needed extra protections for sharing information beyond what is currently available under Protected Critical Infrastructure Information (PCII) provisions.

F. Safe Harbor for Encrypted Information

Although SIFMA has reservations about several aspects of the data breach notification provisions, SIFMA is supportive of the safe harbor in Section 102(b) whereby if the data which is the subject of a breach is "unusable, unreadable, or indecipherable through a security technology" there is a presumption of no reasonable risk. Currently, not all States allow for such a presumption, so a consistent Federal standard for such a presumption would be helpful when assessing a security breach. Our other concerns related to the data breach notification provisions, are set forth in the next section below.

G. Public Education and Awareness

Public education and awareness campaigns have been a critical method of limiting cyber crimes in the financial services industry. Both the SEC and SIFMA members have promoted public awareness of the risk of disclosure of personal information for many years, and SIFMA supports the expansion of any such campaigns and promotions.

IV. SIFMA Concerns With the Proposal

A. Data Breach Notification

SIFMA members are concerned that the data breach notification provisions in the Proposal are unduly burdensome as currently drafted. Although SIFMA believes a preemptive data breach notification standard would serve the industry well, the Federal Trade Commission (FTC) reporting requirements in the Proposal are potentially more burdensome than the existing web of State data breach notifications laws and regulations. SIFMA believes that a reasonable Federal data breach notification standard would help reduce cyber crime and protect individuals and businesses from unnecessary losses. To reach that standard, however, SIFMA believes the Proposal should be changed to incorporate several critical concepts as outlined below.

1. Definition of Security Breach

As proposed, the definition of "Security Breach" is significantly broader than most existing State data breach notification requirements. SIFMA recommends a definition similar to several State laws that would define security breach as "unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person." *See, e.g.,* Fla. Stat. §817.5681(4). SIFMA also asserts that there should be a good faith exception for employees or agents of the firm for businesses purposes so long as there is no further unauthorized disclosure or use of such information. *See, e.g.,* N.Y. GBS. LAW §899-aa.

2. Definition of Sensitive Personally Identifiable Information

SIFMA believes that the current definition of "Sensitive Personally Identifiable Information" is unduly broad and if left unchecked would increase compliance costs severely without preventing data breach. Leaving the definition open to FTC interpretation and rulemaking creates additional uncertainty. The definition in the Proposal includes a social security number or driver's license number without any other information. Existing State laws generally define "personal information" as a person's name or other identifying information in conjunction with a social security or driver's license number. *See, e.g.,* Fla. Stat. §817.5681(5). The disclosure of a social security or driver's license number without any other identifying information should not trigger data breach notification requirements because such information has limited or no value. Requiring firms to undergo a risk assessment and FTC report every time such a piece of information is misdirected in good faith would require multiple reports per week.

In addition, the definition in Section 1(g)(4) of the Proposal also includes "a unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code." Yet, Section 1(g)(5) requires such information in (g)(4) plus a name or security code to trigger the notification requirements. SIFMA proposes deleting paragraph (g)(4) as duplicative and unnecessarily broad. If section (g)(4) is passed as written, the daily business ramifications for SIFMA member firms would be extensive. Among others, account numbers are necessary for financial firms to transact its business as well as for allocation to ensure that transactions are aligned with proper account information. If transaction information is misdelivered and happens to contain only account numbers, the firm would have to conduct a risk assessment and report the results to the FTC. Those efforts would far outweigh any benefit reaped from such an innocuous disclosure.

3. FTC Reporting Requirements (Safe Harbor Exemption)

The Proposal's exemption under Sec. 102(b) provides a safe harbor from enforcement when a firm determines that there is no risk of harm to an individual from a security breach. The qualifying firm will not send a notice to that individual if within 45 days the firm submits to the FTC a written risk assessment justifying the conclusion of no harm. SIFMA believes that performing a risk assessment and submitting such results to the FTC for every Security Breach no matter how small or insignificant mitigates the potential benefit of having such a safe harbor. As currently drafted, even a small data misdirection between financial institutions due to

an error would constitute a Security Breach and thus would require the firm to perform a risk assessment and submit the results to the FTC. This result is in spite of the fact that the "unauthorized party" is in fact another financial institution covered by the same legal, regulatory and operational controls and there with only minimal risk for harm to the customer. Consequently SIFMA believes that this provision is not actually a safe harbor, but rather an additional layer of reporting obligation. We would recommend that this provision be amended to only cover material Security Breaches, such that a small or insignificant misdirection of data, particularly when the recipient is a regulated entity, should not trigger these requirements.

4. Effective Date

SIFMA members are concerned that the effective date of 90 days after enactment for the data breach notification requirement is too short. The time frame does not give the FTC adequate time to propose and adopt clarifying regulations. In addition, firms must make corresponding changes to policies and procedures, as well as modify their reporting systems. The new notification and disclosure provisions will require training and hiring of new staff, which will be difficult to achieve in a 90-day period.

B. Covered Critical Infrastructure

1. DHS as a Cybersecurity Regulator

As currently drafted, the Proposal centralizes domestic cybersecurity responsibilities in DHS, thus making DHS a regulator as well as an enforcer. The addition of DHS into the web of financial services regulation may cause complications for both regulators and regulated financial services firms. SIFMA would prefer for the existing financial regulators to continue as primary regulators for the firms. The financial regulators could then coordinate with DHS and the FTC to the extent necessary, but the firms would not be required to report directly to DHS.

DHS is primarily a technical coordination agency for cybersecurity but DHS has no fundamental understanding of the many business functions performed by the financial services sector. Sector Specific Agencies (SSAs), such as the Department of Treasury, under Homeland Security Presidential Decision Directive 7 and the National Infrastructure Protection Plan, play a significant role for the sector in providing business understanding and advocacy.

In addition, there is a technical capability gap between DHS, the NSA, and U.S. Cyber Command (CYBERCOM). NSA, CYBERCOM, and all intelligence community members need to be subordinate technical and operational resources that DHS coordinates to support critical infrastructure. These agencies need to be subject to the mandate of the National Infrastructure Protection Plan (NIPP) and function to coordinate all engagement with CI/KR sectors through DHS and the SSAs. DHS would be responsible for the incident response process and national technical coordination. For the financial services industry, the Department of Treasury, along with the SEC, CFTC, Federal Reserve Board, and others, would handle mission, business, and regulatory coordination.

2. Identifying Critical Infrastructure Operators

The Proposal gives DHS the authority to designate an organization as a critical infrastructure operator. SIFMA believes that DHS is not well-suited to this role because of its lack of familiarity with the operations of financial services organizations. The Treasury Department, as the Sector Specific Agency for the financial services sector, and the regulatory agencies through the FBIIC, should determine if an institution in the sector is considered critical, not DHS.

3. Risk Mitigation Framework and Evaluation

The Proposal would require critical operators to develop a framework to address cyber threats, and engage a third-party commercial auditor to assess such plans. These requirements would impose significant additional administrative burdens on financial services firms which are already subject to intense regulation. Although engaging an independent auditor significantly increases defense against cyber threats, it does not guarantee effectiveness. It also appears that DHS and NIST would have the ability to modify a firm's framework, which raises many questions for SIFMA members.

4. Public Disclosure of Cybersecurity Plans

SIFMA is also concerned about the requirements in the Proposal under Section 7(b) which would require the critical infrastructure operators to publicly disclose high-level summaries of their cybersecurity plans and whether those plans are working effectively. SIFMA believes that any disclosure of cyber defensive mecha-

nisms may give criminals information which may help them to carry out a cyber crime.

V. Conclusion

SIFMA supports the efforts of President Obama and Congress to further protect the American people, businesses, and Government from the increasing threat of cyber attacks and cyber crimes. SIFMA believes that this Proposal could help achieve those goals if the amendments suggested in this statement are implemented. Without such changes, this Proposal will have diminished value and could do more harm than good for SIFMA members and their customers.